

جامعة ميد أوشن



كلية الإدارة

تخصص إدارة المخاطر

أثر المخاطر الإلكترونية على أداء المنظمة دراسة تطبيقية على شركات

التقنية بمدينة الرياض

إعداد الطالب/

عمّار فهد التميمي

242001099

إشراف/

د. عماد النخلي

العام الدراسي:

2025 – 1446



إهداء

إلى أظهر قلبين في حياتي... والديّ العزيزين.

إلى من شاركني السراء والضراء، ولم أرها عابسة يوماً.... زوجتي

المخلصة.

إلى من أتشوق لأن أرى مستقبلهما المشرق بإذن الله..... ابنتيّ الغاليتين.

إلى جموع الأقارب والأصدقاء

أهديكم بحثي، وأدعو الله أن يحوز إعجابكم.



نحمد الله عز وجل الذي وفقنا في إتمام هذا البحث العلمي،
والذي ألهمنا الصحة والعافية والعزيمة.

فالحمد لله حمدا كثيرا
نتقدم بجزيل الشكر والتقدير إلي الأستاذ الدكتور /
د. عماد النخلي

على كل ما قدمه لنا من توجيهات ومعلومات قيمة ساهمت في
إثراء موضوع دراستنا في جوانبها المختلفة.
والشكر والتقدير موصول إلي إدارة جامعة ميد أوشن ممثلة بالكادر
الأكاديمي والإداري، لما قدموه من تسهيلات وتشجيع وتوفير
الخدمات المطلوبة.

كما أتقدم بالشكر الجزيل لكل من لم يسعنا الحظ بذكر أسمائهم
راجيا من المولي عز وجل أن تكون هذه الدراسة نافذة لدراسات
أخرى .

المستخلص

هدفت هذه الدراسة إلى تحليل أثر المخاطر الإلكترونية بأبعادها (مخاطر أمن المعلومات، مخاطر الاحتيال، ومخاطر عدم رضا العملاء) على أداء الشركات في شركات التقنية بمدينة الرياض، ولتحقيق أهداف الدراسة، تم استخدام المنهج الوصفي التحليلي، وتم توزيع 370 استبانة على عينة عشوائية بسيطة من العاملين في شركات التقنية بمدينة الرياض، وقد تم استرداد 318 استبانة صالحة للتحليل بنسبة استرداد بلغت 85.9%.

أظهرت النتائج أن أبعاد المخاطر الإلكترونية الثلاثة تؤثر بشكل دال إحصائيًا على أداء الشركات. حيث تبين أن مخاطر عدم رضا العملاء كانت الأعلى تأثيرًا، تليها مخاطر الاحتيال، ثم مخاطر أمن المعلومات، وأوصت الدراسة بضرورة تطوير سياسات أمن معلومات متقدمة، وتعزيز نظم كشف الاحتيال، وتحسين إدارة علاقات العملاء للحد من مخاطر عدم رضاهم، إضافة إلى رفع الوعي السيبراني على جميع مستويات المؤسسة، وذلك لضمان أداء تنظيمي مستدام في ظل البيئة الرقمية المتغيرة.

الكلمات المفتاحية: المخاطر الإلكترونية، أمن المعلومات، الاحتيال الإلكتروني، رضا العملاء، أداء

الشركات، شركات التقنية.

قائمة المحتويات

أ.....	بسم الله الرحمن الرحيم
ب.....	الإهداء
ج.....	الشكر والتقدير
د.....	المستخلص
ه.....	قائمة المحتويات
ط.....	قائمة الجداول
1.....	الفصل الأول: الإطار العام للدراسة
1.....	مقدمة:
3.....	1.1 مشكلة الدراسة:
4.....	2.1 أهمية الدراسة:
4.....	أولاً: الأهمية العلمية
4.....	ثانياً: الأهمية العملية
5.....	3.1 أهداف الدراسة:
5.....	4.1 تساؤلات الدراسة:
6.....	5.1 فروض الدراسة:
6.....	6.1 الدراسات السابقة:
12.....	7.1 الفجوة البحثية
14.....	8.1 المنطلقات النظرية للدراسة:

9.1 المنهجية وطرق البحث:	15
10.1 مصادر جمع البيانات:	15
11.1 أدوات الدراسة:	16
12.1 الأساليب الإحصائية المستخدمة:	16
13.1 حدود الدراسة:	17
الفصل الثاني: الإطار النظري:	18
المبحث الأول: المخاطر الإلكترونية:	18
المقدمة:	18
1.1.2 مصادر المخاطر الإلكترونية:	20
2.1.2 أهداف المخاطر الإلكترونية:	22
3.1.2 مجالات الخطر الإلكتروني:	22
4.1.2 صور المخاطر الإلكترونية:	23
5.1.2 أهمية المخاطر الإلكترونية في العصر الرقمي:	24
6.1.2 أنواع المخاطر الإلكترونية:	26
7.1.2 الوقاية والحماية من المخاطر الإلكترونية:	28
المبحث الثاني: أداء المنظمة:	31
المقدمة:	31
1.2.2 أداء المنظمة: مفاهيم أساسية:	31
2.2.2 ثانيا: تصنيفات الأداء ومستوياته:	34
3.2.2 مستويات الأداء:	38

39.....	4.2.2 محددات الأداء ومعوقاته:
40.....	5.2.2 أبعاد الأداء:
41.....	6.2.2 العوامل المؤثرة في أداء المنظمة:
45.....	7.2.2 قياس وتحسين وتقييم الأداء:
48.....	الفصل الثالث: منهجية الدراسة وإجراءاتها
48.....	تمهيد:
48.....	1.3 منهج الدراسة:
48.....	2.3 مجتمع البحث وعينته:
49.....	3.3 أداة الدراسة:
49.....	4.3 بناء أداة الدراسة:
50.....	5.3 صدق أداة الدراسة:
51.....	6.3 ثبات أداة الدراسة:
52.....	7.3 أساليب تحليل البيانات:
54.....	الفصل الرابع: نتائج الدراسة وتفسيرها
54.....	المقدمة:
54.....	1.4 خصائص عينة الدراسة:
56.....	2.4 دراسة محاور الاستبيان:
56.....	المحور الأول المخاطر الإلكترونية
62.....	المحور الثاني أداء شركات
64.....	3.4 فرضيات الدراسة:

69.....	الفصل الخامس : النتائج والتوصيات
69.....	1.5 نتائج الدراسة.....
70.....	2.5 نتائج اختبار الفرضيات.....
72.....	3.5 توصيات الدِّراسة.....
74.....	Abstract.....
75.....	المراجع.....
75.....	أولاً: المراجع العربية.....
78.....	ثانياً: المراجع الأجنبية.....
81.....	الملاحق.....
82.....	استمارة استبيان.....

قائمة الجداول

رقم الجدول	اسم الجدول	رقم الصفحة
1.	جدول رقم (1) مفتاح التصحيح	50
2.	جدول (2) معاملات الارتباط لمحور المخاطر الإلكترونية :	51
3.	جدول (3) معاملات الفا كرونباخ لمحاور الدراسة	52
4.	جدول (4): توزيع أفراد عينة الدراسة حسب الخصائص الديموغرافية (حجم العينة = 318)	54
5.	جدول (5) المتوسطات الحسابية والانحرافات المعيارية والترتيب لعبارات بعد مخاطر أمن المعلومات	56
6.	جدول (6) المتوسطات الحسابية والانحرافات المعيارية والترتيب لعبارات بعد مخاطر الاحتيال	58
7.	جدول (7) المتوسطات الحسابية والانحرافات المعيارية والترتيب لعبارات بعد مخاطر عدم رضا العملاء	60
8.	جدول (8) المتوسطات الحسابية والانحرافات المعيارية والترتيب لعبارات المحور الثاني	62
9.	جدول (9) أثر المخاطر الإلكترونية على أداء شركات في شركات التقنية بمدينة الرياض	64
10.	جدول (10) أثر بعد مخاطر أمن المعلومات على أداء شركات في شركات التقنية بمدينة الرياض	66

67	جدول (11) أثر لبعد مخاطر الاحتيال على أداء شركات في شركات التقنية بمدينة الرياض ..	.11
67	جدول (12) أثر لبعد مخاطر عدم رضا العملاء على أداء شركات في شركات التقنية بمدينة الرياض	.12

الفصل الأول: الإطار العام للدراسة

مقدمة:

أدى التوسع في استخدام التقنيات الرقمية في مختلف قطاعات الأعمال إلى ظهور تحديات جديدة، لعل أبرزها ما يُعرف بـ"المخاطر الإلكترونية"، وهي المخاطر المرتبطة باستخدام تكنولوجيا المعلومات والاتصالات، وما ينجم عنها من تهديدات للأمن السيبراني، وسرية المعلومات، واستمرارية الأعمال. ومع تعاظم دور البيانات والأنظمة الرقمية، أصبحت هذه المخاطر تمثل مصدر قلق متزايد للمنظمات على مستوى العالم، لما لها من تأثير مباشر على البنية التحتية الرقمية والعمليات التشغيلية الحساسة.

(Dorairajan, 2024)

تتنوع المخاطر الإلكترونية في صور متعددة، أبرزها مخاطر أمن المعلومات التي تشمل محاولات اختراق البيانات أو تسريبها أو تعديلها، ومخاطر الاحتيال الإلكتروني التي تشمل استخدام وسائل غير مشروعة لتحقيق مكاسب مادية، بالإضافة إلى مخاطر تؤثر على رضا العملاء نتيجة تجارب رقمية غير آمنة أو ضعف استجابة الشركات للحوادث السيبرانية. ويزداد الأمر تعقيداً في بيئات العمل التقنية التي تتسم بدرجة عالية من الترابط بين الأنظمة والمنصات والخدمات (Quinn et al., 2023).

وفي ظل التحول الرقمي المتسارع، لم تعد المخاطر الإلكترونية تُعد مجرد تهديد أمني، بل تحولت إلى عامل استراتيجي يجب على المؤسسات أخذه بعين الاعتبار ضمن خططها الإدارية والتشغيلية. فقد أصبح من الضروري إدارة هذه المخاطر ضمن إطار متكامل يشمل التقنية، والموارد البشرية، والثقافة المؤسسية، لضمان التكيف مع التحديات، وتحقيق المرونة التنظيمية في بيئة تتسم بالتغير المستمر.

(Hasan et al., 2021)

في المقابل، يُعد أداء الشركات من أكثر المؤشرات الحيوية التي تعكس كفاءة المؤسسة وفعاليتها في تحقيق أهدافها الاستراتيجية والتشغيلية. ويتجسد الأداء من خلال مجموعة من المؤشرات المالية وغير

المالية، مثل الربحية، الكفاءة التشغيلية، الابتكار، جودة الخدمة، رضا العملاء، والقدرة على المنافسة في السوق. ويُستخدم هذا المفهوم بشكل أساسي لتقييم مدى قدرة المؤسسة على التفاعل مع البيئة الداخلية والخارجية بكفاءة (Faisal, 2018).

يرتبط أداء الشركات بعدة عوامل داخلية وخارجية، من بينها البنية التنظيمية، القيادة، التكنولوجيا، والموارد البشرية. لكن في ظل البيئة الرقمية الحالية، أصبح من الضروري النظر إلى عوامل جديدة مثل التهديدات السيبرانية والجهازية الرقمية، كونها تساهم بشكل مباشر في رفع أو خفض مستويات الأداء، وذلك وفقًا للقدرة المؤسسية على مواجهتها واحتوائها ضمن منظومة الحوكمة المؤسسية. (Hasan et al., 2021)

كما أن الأداء التنظيمي لا يعتمد فقط على الكفاءة التشغيلية، بل أيضًا على المرونة في الاستجابة للآزمات والمخاطر، وخاصة المخاطر الإلكترونية التي قد تؤدي إلى توقف الأعمال، أو تراجع ثقة العملاء، أو تكبد خسائر مالية جسيمة، مما يجعل إدارة الأداء في العصر الرقمي أكثر تعقيدًا وتطلبًا لاستراتيجيات متكاملة تتعامل مع التهديدات المستجدة (Dorairajan, 2024).

وعليه، فإن العلاقة بين المخاطر الإلكترونية وأداء الشركات أصبحت محل اهتمام متزايد من الباحثين والممارسين، حيث تشير الأدبيات إلى أن التهديدات السيبرانية قد تُحدث تأثيرات مباشرة وغير مباشرة على الأداء، تبدأ من انخفاض رضا العملاء، مرورًا بتزايد التكاليف التشغيلية، ووصولًا إلى تهديد الاستمرارية المؤسسية. ومن هنا، تتطلب بيئة الأعمال الرقمية إدارة متكاملة للمخاطر لضمان تحسين الأداء المؤسسي (Quinn et al., 2023).

في ضوء ما سبق، تبرز الحاجة إلى دراسة العلاقة بين أبعاد المخاطر الإلكترونية (أمن المعلومات، الاحتيال، عدم رضا العملاء) وأداء الشركات، وبخاصة في بيئة الشركات التقنية بمدينة الرياض، التي تُعد من أكثر القطاعات عرضة لهذه التهديدات.

1.1 مشكلة الدراسة:

شهد العالم خلال العقدین الماضیین تطورًا هائلًا في استخدام التقنیات الرقمية، وازدادت وتيرة التحول الرقمي في مختلف القطاعات، ولا سيما في شركات التقنية التي تعتمد بصورة جوهريّة على الأنظمة الإلكترونية في تنفيذ عملياتها التشغيلية والإدارية. هذا التوسع في الرقمنة، وإن كان يمثل فرصة لتعزيز الكفاءة والابتكار، إلا أنه أدى إلى نشوء تحديات أمنية وتنظيمية معقدة تمثلت في المخاطر الإلكترونية، التي باتت تشكل تهديدًا متزايدًا لاستمرارية الأعمال، وفاعلية الأداء المؤسسي (Dorairajan, 2024)؛ Hasan (et al., 2021).

وتتعدد أبعاد المخاطر الإلكترونية، وتشمل بشكل خاص: مخاطر أمن المعلومات، الناتجة عن اختراقات أو تسريبات في البيانات الحساسة، ومخاطر الاحتيال الإلكتروني، الناتجة عن استغلال الثغرات الرقمية لارتكاب أعمال غير مشروعة، بالإضافة إلى مخاطر عدم رضا العملاء، التي تنتج عن انخفاض جودة الخدمات الرقمية أو ضعف الاستجابة للمشكلات التقنية (Quinn et al., 2023)؛ (Adeb, 2019) وتشير الأدبيات إلى أن هذه المخاطر قد تؤثر بصورة مباشرة أو غير مباشرة على الأداء التنظيمي من حيث الكفاءة التشغيلية، والمرونة، والقدرة التنافسية (Hasan et al., 2021)؛ (Dorairajan, 2024).

وعلى الرغم من تزايد أهمية الأمن السيبراني، فقد لوحظ أن معظم الدراسات السابقة تناولت المخاطر الإلكترونية من منظور تقني أو أممي فقط، دون الربط الصريح أو المباشر بينها وبين أداء الشركات التنظيمي، خصوصًا في بيئة الأعمال التقنية داخل الدول العربية، ومنها المملكة العربية السعودية. كما أن عددًا محدودًا من الدراسات (مثل دراسة Hasan et al., 2021) تناول العلاقة بين الجاهزية السيبرانية والأداء، لكن دون التعمق في تحليل أثر كل بُعد من أبعاد المخاطر الإلكترونية على الأداء المؤسسي بشكل منفصل.

وبناءً على ما سبق، تتحدد مشكلة الدراسة في التساؤل الرئيس الآتي: ما أثر المخاطر الإلكترونية بأبعادها الثلاثة (مخاطر أمن المعلومات، ومخاطر الاحتيال، ومخاطر عدم رضا العملاء) على أداء الشركات في شركات التقنية بمدينة الرياض؟

2.1 أهمية الدراسة:

تكتسب هذه الدراسة أهمية كبيرة من الناحيتين العلمية والعملية، حيث تستهدف تسليط الضوء على أثر المخاطر الإلكترونية على أداء شركات التقنية، خاصة في مدينة الرياض التي تعتبر مركزاً رئيسياً للابتكار الرقمي في المملكة العربية السعودية. مع التطور السريع في مجال التكنولوجيا والتحول الرقمي المتسارع، أصبحت المخاطر الإلكترونية تهديداً حقيقياً يواجه الشركات، مما يجعل من الضروري فهم هذه المخاطر وتأثيرها على الأداء العام للشركات. تتنوع أهمية الدراسة إلى بعدين رئيسيين هما الأهمية العلمية والأهمية العملية.

أولاً: الأهمية العلمية

تسهم الدراسة في إثراء المعرفة العلمية المتعلقة بالمخاطر الإلكترونية وأثرها على أداء الشركات، حيث توفر إطاراً علمياً متكاملًا يساعد الباحثين والمهتمين بمجال الأمن السيبراني وإدارة المخاطر في فهم العلاقة بين المخاطر الإلكترونية وأداء الشركات التقنية. تركز الدراسة على أبعاد محددة للمخاطر الإلكترونية، مثل مخاطر أمن المعلومات، ومخاطر الاحتيال، ومخاطر عدم رضا العملاء، وتحليل كيفية تأثير كل من هذه المخاطر على أبعاد الأداء التنظيمي، والتي تشمل الأداء المالي، الأداء التشغيلي، ورضا العملاء. من خلال ذلك، تساعد الدراسة على سد الفجوة المعرفية في الأدبيات الأكاديمية حول هذا الموضوع، مما يوفر أساساً لدراسات مستقبلية تسعى لفهم تأثير المخاطر الرقمية على قطاعات أخرى متنوعة. كما تقدم نموذجاً علمياً يمكن للباحثين البناء عليه وتطويره، مما يعزز من تطوير السياسات الأكاديمية والاستراتيجيات المرتبطة بإدارة المخاطر الإلكترونية.

ثانياً: الأهمية العملية

تمثل هذه الدراسة دليلاً عملياً لصناع القرار والمديرين في شركات التقنية بمدينة الرياض، حيث تقدم نتائج وتوصيات قابلة للتطبيق تساعد على مواجهة المخاطر الإلكترونية المتزايدة. من خلال فهم تأثير هذه المخاطر على الأداء المالي والتشغيلي للشركات، وكذلك على رضا العملاء، توفر الدراسة أدوات

عملية تساعد في تحسين الأداء العام للشركات وتعزيز قدرتها التنافسية. تدعم نتائج الدراسة الشركات في تطوير سياسات أمنية قوية وإجراءات وقائية تحد من مخاطر أمن المعلومات ومخاطر الاحتيال، بالإضافة إلى تحسين استراتيجيات الحفاظ على رضا العملاء من خلال تحسين التجربة الرقمية الآمنة للعملاء.

تساعد الدراسة الشركات في تعزيز وعيها بأهمية إدارة المخاطر الإلكترونية وتأثيرها المباشر على مستوى الثقة لدى العملاء. حيث تمثل المخاطر الإلكترونية تحدياً معقداً يهدد الثقة بين الشركة وعملائها. بالتالي، فإن تطبيق سياسات وإجراءات قوية للأمن السيبراني بناءً على نتائج هذه الدراسة يمكن أن يساهم في رفع مستوى الثقة لدى العملاء، مما يساهم في تعزيز تنافسية الشركات في سوق التكنولوجيا المتنامي.

3.1 أهداف الدراسة:

- تهدف الدراسة إلى التعرف على أثر المخاطر الإلكترونية بأبعادها (مخاطر أمن المعلومات، مخاطر الاحتيال، مخاطر عدم رضا العملاء) على أداء شركات التقنية بمدينة الرياض بأبعاده (الأداء المالي، الأداء التشغيلي، رضا العملاء)، وتتفرع منه عدة أهداف فرعية:
- التعرف على أثر مخاطر أمن المعلومات على أداء شركات التقنية بمدينة الرياض .
- التعرف على أثر مخاطر الاحتيال على أداء شركات التقنية بمدينة الرياض .
- التعرف على أثر مخاطر عدم رضا العملاء على أداء شركات التقنية بمدينة الرياض .

4.1 تساؤلات الدراسة

ما هو أثر المخاطر الإلكترونية بأبعادها (مخاطر أمن المعلومات، مخاطر الاحتيال، مخاطر عدم رضا العملاء) على أداء شركات التقنية بمدينة الرياض بأبعاده (الأداء المالي، الأداء التشغيلي، رضا العملاء)؟

الأسئلة الفرعية

- السؤال الفرعي الأول: ما هو أثر مخاطر أمن المعلومات على أداء شركات التقنية بمدينة الرياض ؟
- السؤال الفرعي الثاني: ما هو أثر مخاطر الاحتيال على أداء شركات التقنية بمدينة الرياض ؟

- السؤال الفرعي الثالث: ما هو أثر مخاطر عدم رضا العملاء على أداء شركات التقنية بمدينة الرياض؟

5.1 فروض الدراسة:

الفرضية الرئيسية H_0 : لا يوجد أثر ذو دلالة إحصائية عند مستوى $(\alpha \leq 0.05)$ للمخاطر الإلكترونية على أداء شركات التقنية بمدينة الرياض. ويتفرع من هذه الفرضية مجموعة الفرضيات الفرعية التالية:

- الفرضية الفرعية الأولى (H_{02}): لا يوجد أثر ذو دلالة إحصائية عند مستوى الدلالة $(\alpha < 0.05)$ لمخاطر أمن المعلومات على أداء شركات التقنية بمدينة الرياض.
- الفرضية الفرعية الثانية (H_{03}): لا يوجد أثر ذو دلالة إحصائية عند مستوى الدلالة $(\alpha < 0.05)$ لمخاطر الاحتيال على أداء شركات التقنية بمدينة الرياض.
- الفرضية الفرعية الثالثة (H_{04}): لا يوجد أثر ذو دلالة إحصائية عند مستوى الدلالة $(\alpha < 0.05)$ لمخاطر عدم رضا العملاء على أداء شركات التقنية بمدينة الرياض.

6.1 الدراسات السابقة:

■ دراسة (Dorairajan (2024

هدفت الدراسة إلى التعرف على التفاعل بين الأمن السيبراني والأداء التنظيمي، من خلال دراسة كيفية تأثير الأمن السيبراني على مقاييس الأداء التنظيمي وكيف يتأثر بها. تناولت الدراسة عدة أبعاد تتعلق بالأمن السيبراني (حماية سرية المعلومات، سلامة الأصول الرقمية، الثقافة السيبرانية، العوامل البشرية) وأبعاد الأداء التنظيمي (إدارة المخاطر، الامتثال، الأداء المالي). كما تم التركيز على إطار العمل التقني-المنظمي-البيئي (TOE framework)، حيث شمل السياق التكنولوجي (التكلفة، العائد، التعقيد)، والسياق

التنظيمي (الدعم الإداري، الجاهزية، الخبرة)، والسياق البيئي (التنافسية، القوانين واللوائح، الأحداث الخارجية).

استخدمت الدراسة منهجية تحليلية نظرية لاستكشاف العلاقة بين الأمن السيبراني والأداء التنظيمي، وناقشت كيفية تأثير الرقمنة والتحول الرقمي على ثقافة المؤسسات نحو الأمن السيبراني. كما بينت الدراسة أن التنظيمات التي تتبنى إجراءات أمنية استباقية يمكنها تحسين الثقة بين شركائها التجاريين، مما يعزز القدرة التنافسية ويسهم في تيسير المعاملات التجارية.

أظهرت النتائج أن الأمن السيبراني أصبح ينظر إليه كعامل دعم للنمو والتنافسية بدلاً من كونه عبئاً مالياً، مما يعزز الكفاءة التشغيلية والثقة. كما أكدت الدراسة على أهمية تبني نموذج التوازن بين الأمن والأداء (Security-Performance Tradeoff Model)، والذي يتناول ضرورة تحقيق توازن بين مستوى الأمان والأداء التشغيلي دون التأثير السلبي على تجربة المستخدم. أوصت الدراسة بتبني نهج قائم على الأولويات في إدارة المخاطر، وتطوير إطار أمني متكيف مع التهديدات المتغيرة، وتعزيز الوعي بالأمن السيبراني على جميع مستويات المؤسسة.

■ دراسة (Quinn et al., 2023)

هدفت الدراسة إلى التعرف على تأثير مخاطر تكنولوجيا المعلومات والاتصالات (ICT) على مستوى المؤسسة، مع التركيز على دمج هذه المخاطر في برامج إدارة المخاطر المؤسسية (ERM). تناولت الدراسة أبعاد إدارة مخاطر ICT (التحديد، التقييم، الإدارة) وأبعاد التأثير المؤسسي (التوافق مع الأهداف المؤسسية، الدعم عبر مستويات النظام، تكامل إدارة المخاطر على مستوى المؤسسة). ركزت الدراسة على أهمية استخدام سجلات مخاطر ICT كمدخل لتشكيل صورة متكاملة لمخاطر المؤسسة، مما يساعد في تحسين القدرة على تحديد وتقييم وإدارة مخاطر ICT بشكل فعال في سياق أهداف المؤسسة الأكبر.

اعتمدت الدراسة على منهجية وصفية تحليلية لدراسة كيفية تأثير إدراج إدارة مخاطر ICT ضمن إطار ERM في تعزيز التكامل المؤسسي، وتم تطبيق البحث على عينة من المؤسسات الكبيرة التي تعتمد بشكل مكثف على أنظمة تكنولوجيا المعلومات والاتصالات في عملياتها.

أظهرت النتائج أن دمج سجلات مخاطر ICT ضمن برامج ERM يضيف قيمة كبيرة، حيث يساهم في تحسين الوعي المؤسسي بالمخاطر ويساعد في تخصيص الموارد بشكل أكثر فعالية. وأوصت الدراسة بضرورة إعطاء أهمية أكبر لمخاطر ICT ضمن استراتيجيات إدارة المخاطر المؤسسية، وتبني سياسات واضحة تدعم التكامل بين المستويات التشغيلية والتنظيمية لتحقيق أهداف المؤسسة بشكل آمن ومستدام.

■ دراسة (Hasan et al., 2021)

هدفت الدراسة إلى تقييم جاهزية الأمن السيبراني لدى المنظمات وتأثيرها على الأداء التنظيمي، حيث تركزت الدراسة على تحليل كيفية استعداد المنظمات لمواجهة الهجمات السيبرانية وتأثير ذلك على أدائها المالي وغير المالي. اعتمدت الدراسة على إطار العمل التقني-المنظمي-البيئي (TOE) ، الذي يشمل أبعاد جاهزية الأمن السيبراني (العوامل التكنولوجية، العوامل التنظيمية، العوامل البيئية) كمتغيرات رئيسية، وتأثير هذه الجاهزية على الأداء الأمني للمؤسسة، ومن ثم تأثير الأداء الأمني على الأداء المالي وغير المالي.

استخدمت الدراسة منهجية كمية من خلال استبيان موجه إلى محترفي تكنولوجيا المعلومات في البحرين، وتم جمع 270 استجابة صالحة. وقد أظهرت النتائج أن جاهزية الأمن السيبراني تؤثر بشكل إيجابي على الأداء الأمني للمؤسسة، مما يؤثر بدوره على الأداء المالي وغير المالي. كما تم تأكيد أهمية سبعة من بين تسعة عوامل تؤثر على جاهزية الأمن السيبراني، والتي سبق أن تم تحديدها في دراسات سابقة.

أوصت الدراسة باستخدام النموذج الشامل المقترح كمرجع للبحوث المستقبلية، حيث يمكن أن يساهم في تحسين فهم كيفية تجهيز المنظمات لمواجهة التحديات السيبرانية وتقليل آثارها السلبية على الأداء العام، وبالتالي تعزيز استراتيجيات الأمن السيبراني لتحقيق أداء مؤسسي مستدام.

■ دراسة (صبيح، 2021)

هدفت الدراسة إلى استكشاف المخاطر المرتبطة بالتسويق الرقمي عبر مواقع التسوق الإلكتروني من وجهة نظر المراهقين، بالإضافة إلى تحليل تأثير هذه المخاطر على أنماط السلوك الاستهلاكي لديهم. ركزت الدراسة على عناصر متعددة ضمن التسويق الرقمي (طريقة الترويج، محتوى المنتج، الإعلانات، الخصومات والعروض، التوزيع، السعر، المنتج) لتقييم المخاطر المحتملة وتأثيرها على الأنماط المختلفة لسلوك المستهلك (المستهلك العقلاني، المستهلك المندفع، المستهلك المتردد، المستهلك المترث، المستهلك الجاهل، المستهلك الثرثار). اعتمدت الدراسة المنهج الوصفي التحليلي واستخدمت عينة من المراهقين لتحليل البيانات وتحديد أنماط استجاباتهم تجاه هذه المخاطر. أظهرت النتائج أن أكثر عناصر التسويق الرقمي المحفزة للسلوك الاستهلاكي كانت طريقة الترويج، محتوى المنتج، والإعلانات، مع ميل المراهقين نحو السلوك الاستهلاكي العقلاني يليه السلوك المندفع. وكشفت الدراسة عن وجود فروق ذات دلالة إحصائية في أنماط السلوك الاستهلاكي تبعًا لعوامل المستوى الاجتماعي الاقتصادي للأسرة، نوع التعليم، والمرحلة الثانوية. أوصت الدراسة بضرورة توعية المراهقين بمخاطر التسويق الرقمي عبر مواقع التسوق الإلكتروني، وتفعيل دور الأسرة والمدرسة في توجيه سلوك المراهقين نحو استخدام آمن وفعال للتكنولوجيا، مع وضع ضوابط قانونية وأخلاقية لحماية المراهقين من مخاطر التسويق الرقمي.

■ دراسة (عزوز، 2019)

هدفت الدراسة إلى قياس أثر استراتيجيات تخفيض المخاطر المدركة للتسويق الإلكتروني على القرار الشرائي للمستهلك المصري عبر شبكات التواصل الاجتماعي، مع التركيز على تأثير ارتفاع ظاهرة الخداع التسويقي وانخفاض دور أجهزة حماية المستهلك على سلوك الشراء. اشتملت الدراسة على استراتيجيات تخفيض المخاطر (اللجوء للعلامة التجارية، وثيقة الضمان، المنتجات أو الخدمات الأعلى سعرًا) كمحاور أساسية، بينما شمل القرار الشرائي (اتخاذ القرار الشرائي، الولاء للعلامة التجارية). استخدمت الدراسة المنهج الوصفي التحليلي وطبقت على عينة من المستهلكين المصريين. أظهرت النتائج أن استراتيجيات تخفيض المخاطر، وبالأخص الولاء للعلامة التجارية، كانت الأكثر تأثيرًا على قرار الشراء، حيث

ساهمت في تعزيز الثقة في الشراء عبر الإنترنت. وأوصت الدراسة بتوعية المستهلك المصري بمخاطر التسويق الإلكتروني، وتعزيز ثقافة الشراء الآمن عبر الإنترنت، وتفعيل دور أجهزة حماية المستهلك في مراقبة الشركات التي تمارس الخداع التسويقي.

■ دراسة (المتولي، 2018)

هدفت الدراسة إلى دراسة العلاقة بين مراجعات العملاء الإلكترونية ونية حجز الفندق في مصر، مع التركيز على دور المخاطر المدركة كعامل وسيط في هذه العلاقة. تناولت الدراسة أبعاد مراجعات العملاء الإلكترونية (مصادقية المعلومات، سهولة الاستخدام، محتوى المراجعات) كمتغير مستقل، بينما مثلت نية الحجز (رغبة في الحجز، توقع تجربة جيدة) كمتغير تابع. طبقت الدراسة المنهج الوصفي التحليلي على عينة من مستخدمي مواقع الحجز الإلكتروني للفنادق. بينت النتائج وجود علاقة إيجابية بين مصادقية وسهولة استخدام المراجعات الإلكترونية ونية الحجز، بينما كانت هناك علاقة سلبية بين المخاطر المدركة ونية الحجز. أوصت الدراسة بأهمية تحسين إدارة الفنادق لمراجعات العملاء الإلكترونية، وتوفير قنوات سهلة للعملاء لتقديم مراجعاتهم، وتوعية العملاء بالمخاطر وكيفية تقييمها لضمان تجربة حجز آمنة.

■ دراسة (أديب، 2019)

هدفت الدراسة إلى معرفة مدى إدراك الشباب لمخاطر التسوق الإلكتروني في المجتمعات الافتراضية الاستهلاكية، وتحليل العلاقة بين إدراكهم لهذه المخاطر وسلوكهم الشرائي. تناولت الدراسة أبعاد المخاطر الإلكترونية (مخاطر أمن المعلومات، مخاطر الاحتيال، مخاطر عدم رضا العملاء) كمتغير مستقل، بينما شمل السلوك الشرائي (الاتجاه نحو الشراء الإلكتروني، النية السلوكية نحو الشراء الإلكتروني) كمتغير تابع. اعتمدت الدراسة على المنهج الوصفي التحليلي وطبقت على عينة من الشباب في المجتمعات الافتراضية. أظهرت النتائج أن الشباب لديهم إدراك مرتفع للمخاطر، مما يؤثر إيجابياً على توجههم نحو التسوق الإلكتروني بشكل آمن، ولكن له تأثير سلبي على نيتهم الشرائية. وأوصت الدراسة بزيادة الوعي بين الشباب بمخاطر التسوق الإلكتروني، وتوفير بيئة تسوق آمنة وضمانات تحمي حقوق المستهلكين.

■ دراسة (رشوان، 2020)

هدفت الدراسة إلى تحليل تأثير الضغوط المؤسسية على أداء المنظمة في المنظمات الصناعية بمصر، مع التركيز على دور ممارسات إدارة سلسلة التوريد الخضراء كمتغير وسيط في هذه العلاقة. شملت الدراسة أبعاد الضغوط المؤسسية (الضغوط التنظيمية، الضغوط الاجتماعية، الضغوط البيئية) كمتغير مستقل، بينما تناول أداء المنظمة (الأداء المالي، الأداء السوقي، الأداء البيئي) كمتغير تابع. استخدمت الدراسة المنهج الوصفي التحليلي، حيث بينت النتائج وجود تأثير إيجابي للضغوط المؤسسية على أداء المنظمة، إضافة إلى تأثير إيجابي لممارسات إدارة سلسلة التوريد الخضراء كمتغير وسيط. وأوصت الدراسة بتبني ممارسات سلسلة التوريد الخضراء في المنظمات الصناعية، وتوعية العاملين بأهمية الضغوط المؤسسية لتحسين الأداء.

■ دراسة (فيصل، 2018)

هدفت الدراسة إلى فهم العلاقة بين تسويق الخدمات وتحسين أداء المنظمة، وتحديد الدور الوسيط لقدرات المنظمة في هذه العلاقة. تضمنت الدراسة أبعاد تسويق الخدمات (المنتج، السعر، التوزيع، الترويج) كمتغير مستقل، بينما شمل أداء المنظمة (الأداء المالي، الأداء التشغيلي، الأداء التسويقي) كمتغير تابع. اعتمدت الدراسة المنهج الوصفي التحليلي وطبقت على عينة من المنظمات. أظهرت النتائج أن تسويق الخدمات يلعب دورًا كبيرًا في تحسين أداء المنظمة، وأن قدرات المنظمة كانت متغيرًا وسيطًا يعزز هذا التأثير. أوصت الدراسة بتبني استراتيجيات فعالة في تسويق الخدمات، وتعزيز المهارات والتقنيات التي تدعم هذا المجال لرفع الأداء المؤسسي.

■ دراسة (Balishani، 2021)

هدفت الدراسة إلى فهم تأثير مخاطر التسوق الإلكتروني على اتجاهات المستهلكين في الجزائر، وتحديد الأسباب وراء بطء انتشار التسوق الإلكتروني. تناولت الدراسة أبعاد المخاطر (المخاطر الأمنية، المخاطر المالية، مخاطر تتعلق بالمنتج) كمتغير مستقل، بينما كانت اتجاهات المستهلكين نحو التسوق

الإلكتروني (التوجه الإيجابي، التوجه السلبي) هي المتغير التابع. أظهرت النتائج أن المستهلكين الجزائريين لديهم توجه إيجابي نسبياً تجاه التسوق الإلكتروني، رغم إدراكهم للمخاطر. وعزت الدراسة بطء انتشار التسوق الإلكتروني إلى عوامل مثل نقص البنية التحتية وضعف الثقة. وأوصت بضرورة تحسين البنية التحتية وزيادة التوعية لتشجيع التسوق الإلكتروني الآمن.

■ دراسة (Ahmed et al., 2022)

هدفت الدراسة إلى على مدى إدراك الشباب الجامعي للمخاطر المحتملة من التسوق الإلكتروني للمنتجات الدوائية، وتحديد العوامل التي تؤثر على إدراكهم لهذه المخاطر. تناولت الدراسة أبعاد التسوق الإلكتروني للمنتجات الدوائية (الإعلانات، المعلومات، العروض الترويجية) كمتغير مستقل، بينما كان إدراك المخاطر (المخاطر الصحية، المخاطر المالية، المخاطر القانونية) هو المتغير التابع. أوضحت النتائج أن الشباب الجامعيين لديهم وعي مرتفع بالمخاطر المرتبطة بالمنتجات الدوائية عبر الإنترنت، وأن بعض العوامل مثل التخصص وعدد سنوات استخدام الإنترنت تؤثر على هذا الإدراك. وأوصت الدراسة بتكثيف الجهود التوعوية لتوعية الشباب بمخاطر المنتجات الدوائية الإلكترونية، وتقييد الإعلانات غير الموثوقة، وتفعيل الرقابة على هذا النوع من التسوق لحماية حقوق المستهلكين.

7.1 الفجوة البحثية

من خلال استعراض الدراسات السابقة التي تناولت موضوعات الأمن السيبراني، وإدارة مخاطر تكنولوجيا المعلومات والاتصالات، والتسويق الإلكتروني، يتضح أن هناك فجوة بحثية واضحة في الدراسات الحالية. فعلى الرغم من التركيز على أبعاد مختلفة لمخاطر التكنولوجيا وتأثيرها على الأداء التنظيمي، إلا أن الدراسات لم تقدم تكاملاً شاملاً يشمل جميع العوامل البيئية، والتنظيمية، والتكنولوجية، والاجتماعية التي تؤثر على إدارة المخاطر الإلكترونية داخل الشركات الكبرى، وخاصة في القطاعات ذات الحساسية العالية، مثل قطاع الاتصالات وقطاع التقنية.

أولاً: ركزت الدراسات مثل دراسة Dorairajan (2024) و Quinn وآخرون (2023) على أهمية دمج مخاطر تكنولوجيا المعلومات والأمن السيبراني في الاستراتيجيات المؤسسية، مشيرة إلى الأهمية المتزايدة لهذا التكامل في تعزيز الأداء المؤسسي وتعزيز الثقة بين الشركاء التجاريين. ومع ذلك، لم تتناول هذه الدراسات بشكل كافٍ تأثير التكامل بين أبعاد الأمن السيبراني (مثل الثقافة السيبرانية والتفاعل البشري) وبين عناصر أخرى مثل التكنولوجيات الناشئة كالذكاء الاصطناعي وتأثيراتها المتوقعة على الأداء المؤسسي الشامل.

ثانياً: تناولت دراسات مثل Hasan وآخرون (2021) تأثير جاهزية الأمن السيبراني على الأداء المالي وغير المالي، إلا أنها ركزت بشكل كبير على الإطار التكنولوجي التنظيمي البيئي (TOE) كإطار رئيسي دون التوسع في تفسير العوامل الفردية والثقافية وتأثيرها على وعي الموظفين بمخاطر الأمن السيبراني. يبرز هنا نقص في الدراسات التي تربط بين سلوك الأفراد وثقافة المؤسسات في مواجهة المخاطر الإلكترونية وكيفية تعزيز هذا التوجه ليصبح جزءاً لا يتجزأ من الهيكل التنظيمي.

ثالثاً: ركزت بعض الدراسات على التسويق الإلكتروني ومخاطره، مثل دراسة صبيح (2021) ودراسة عزوز (2019)، اللتين تناولتا المخاطر المرتبطة بالتسويق الإلكتروني، إلا أن تلك الدراسات لم تتطرق بشكل كافٍ إلى كيفية دمج إدارة المخاطر الإلكترونية مع استراتيجيات التسويق الإلكتروني لتعزيز الثقة والشفافية مع العملاء وحماية بياناتهم، وهي نقطة هامة تفتقر إليها الأدبيات الحالية في هذا المجال.

أخيراً: توضح الفجوة البحثية أن الدراسات الحالية تحتاج إلى تقديم نموذج شامل ومتكامل يجمع بين أبعاد المخاطر الإلكترونية المختلفة وتأثيراتها على الأداء المؤسسي ضمن بيئات متنوعة ومختلفة التحديات، ويشمل ذلك العوامل الثقافية والتنظيمية والتكنولوجية التي تؤثر في قابلية تبني استراتيجيات الأمن السيبراني في المؤسسات، بالإضافة إلى تأثيراتها على سلوك الموظفين وعلاقتهم بالأمن السيبراني.

بناءً على ذلك، تظهر الحاجة الملحة لإجراء دراسات أعمق تتبنى نهجاً شاملاً لدراسة تأثير المخاطر الإلكترونية على الأداء التنظيمي، مع التركيز على الجوانب البشرية والثقافية والتقنية المتكاملة داخل المؤسسات، والتي تمكن من تطوير استراتيجيات مرنة وفعالة لمواجهة التهديدات السيبرانية المتزايدة.

8.1 المنطلقات النظرية للدراسة:

❖ المخاطر الإلكترونية

المخاطر الإلكترونية تشير إلى التهديدات المحتملة التي قد تؤثر سلباً على الأنظمة والبيانات الرقمية للمؤسسة، وتشمل الأبعاد المتعلقة بأمن المعلومات، الاحتيال الإلكتروني، وعدم رضا العملاء. هذه المخاطر قد تؤثر على سلامة المعلومات وسمعة الشركة، وقدرتها على تقديم خدماتها بفعالية في السوق التقني المتزايد التنافسية (Hasan وآخرون، 2021).

❖ مخاطر أمن المعلومات

تشمل مخاطر أمن المعلومات التهديدات التي تؤثر على سرية وسلامة وتوافر المعلومات الرقمية للمؤسسة، مثل الهجمات السيبرانية التي تهدد البيانات الهامة، وقد يؤدي فشل إدارة هذه المخاطر إلى خسائر مالية وتدهور في سمعة الشركة (Dorairajan، 2024).

❖ مخاطر الاحتيال

تشير مخاطر الاحتيال إلى التهديدات المتعلقة بالتلاعب أو الاستغلال غير المشروع للأنظمة التكنولوجية من قبل الأفراد أو الأطراف الخارجية، مما قد يؤدي إلى خسائر مالية وإضرار بسمعة المنظمة، ويمثل تحدياً كبيراً للشركات في قطاع التقنية (Quinn وآخرون، 2023).

❖ مخاطر عدم رضا العملاء

تشير مخاطر عدم رضا العملاء إلى التهديدات الناتجة عن تراجع تجربة المستخدم وارتفاع مستويات الشكاوى، سواء بسبب مشكلات أمنية أو تقنية، مما يؤثر سلباً على سمعة الشركة وعلاقتها بعملائها، ويضعف من قدرتها التنافسية في السوق (صبيح، 2021).

أداء شركات التقنية: أداء شركات التقنية يمثل قدرة الشركة على تحقيق أهدافها التشغيلية والمالية، ويشمل جوانب متعددة مثل الكفاءة المالية، الكفاءة التشغيلية، ورضا العملاء. الأداء الجيد يعكس فعالية الشركة في إدارة المخاطر وتقديم خدمات ذات جودة عالية (Hasan وآخرون، 2021).

9.1 المنهجية وطرق البحث:

تعتمد هذه الدراسة على المنهج الوصفي التحليلي، الذي يعد منهجاً مناسباً لدراسة أثر المخاطر الإلكترونية بأبعادها المختلفة (مخاطر أمن المعلومات، مخاطر الاحتيال، مخاطر عدم رضا العملاء) على أداء شركات التقنية. يهدف المنهج الوصفي التحليلي إلى وصف الواقع القائم وتحليل العلاقات بين المتغيرات المختلفة وتأثيرها على الأداء التنظيمي، مما يساهم في فهم مدى تأثير الأداء بمختلف المخاطر الإلكترونية.

10.1 مصادر جمع البيانات

❖ المصادر الأولية

تُعتبر المصادر الأولية من أهم أدوات جمع البيانات في هذه الدراسة، حيث سيتم استخدام الاستبانة كأداة رئيسية لجمع المعلومات من المشاركين. سيتم توزيع الاستبانة على عينة من الموظفين والمدراء في هذه الشركات، مما يوفر بيانات مباشرة تعكس تجاربهم وآرائهم. يُتوقع أن تساعد هذه البيانات في تحليل العلاقة بين المتغيرات بشكل دقيق وموثوق.

❖ المصادر الثانوية

بالإضافة إلى المصادر الأولية، سيتم الاستعانة بالمصادر الثانوية لتوفير سياق أكاديمي وأدبي قوي للدراسة. تشمل هذه المصادر الدراسات السابقة، المقالات العلمية، والتقارير المتعلقة بممارسات إدارة الموارد البشرية ونجاح المشاريع. سيتم مراجعة الأدبيات ذات الصلة، مما يساهم في بناء إطار نظري يوجه البحث ويساعد في تفسير النتائج. يُتوقع أن توفر هذه المصادر الثانوية رؤى إضافية تساعد في فهم التوجهات الحالية والتحديات في هذا المجال.

11.1 أدوات الدراسة:

تم استخدام الاستبيان كأداة رئيسية لجمع البيانات، حيث تم تصميم الاستبيان بشكل يغطي كافة الأبعاد المتعلقة بالمخاطر الإلكترونية وأثرها على الأداء. يشتمل الاستبيان على مجموعة من الأسئلة المغلقة التي تقيس كل بعد من أبعاد المخاطر الإلكترونية وأثره على جوانب الأداء المختلفة (الأداء المالي، الأداء التشغيلي، رضا العملاء).

12.1 الأساليب الإحصائية المستخدمة:

لاختبار أسئلة وفرضيات الدراسة والإجابة عنها قام الباحث باستخدام التقنيات الإحصائية للعلوم الاجتماعية SPSS - Statistical Package for Social Sciences كما يلي:

أولاً: أساليب الإحصاء الوصفي Descriptive Statistic Measures: والتي تم استخدامها لوصف الخصائص الديمغرافية والوظيفية للمديرين عينة الدراسة، وتشمل:

- التكرارات: لوصف الخصائص الشخصية والوظيفية للمديرين عينة الدراسة.
- النسب المئوية: تم استخدامها لمعرفة التوزيعات التكرارية لعينة الدراسة.
- المتوسط الحسابي: استخدم لمعرفة متوسط إجابات عينة الدراسة عن فقرات الأبعاد.
- الانحراف المعياري: استخدم لمعرفة تشتت إجابات عينة الدراسة عن المتوسط الحسابي.

ثانياً: الإحصاء التحليلي:

- معامل الثبات كرونباخ الفا: للتعرف على ثبات فقرات ابعاد متغيرات الدراسة.
- الانحدار البسيط: لاختبار أثر المتغير المستقل في المتغير التابع.
- ارتباط بيرسون: للتحقق من صدق أداة الدراسة والتعرف على العلاقة بين المتغيرات

13.1 حدود الدراسة:

- حدود موضوعية : تركيز الدراسة على أبعاد معينة من المخاطر الإلكترونية وهي مخاطر أمن المعلومات، مخاطر الاحتيال، ومخاطر عدم رضا العملاء على أداء المنظمة .
- حدود مكانية: تركز الدراسة على شركات التقنية في مدينة الرياض .
- حدود زمانية: تم إعداد الدراسة في عام 2024.
- حدود بشرية: تقتصر عينة الدراسة على العاملين في شركات التقنية.

الفصل الثاني: الإطار النظري

المبحث الأول: المخاطر الإلكترونية

المقدمة

في عصرنا الحديث، أصبح الإنترنت جزءًا لا يتجزأ من حياتنا اليومية، فهو لا يُستخدم فقط للتواصل والتسلية، بل أصبح عنصرًا أساسيًا في جميع مجالات الحياة، بما في ذلك العمل، التعليم، التجارة، الخدمات المالية، وحتى الرعاية الصحية. ومع تزايد الاعتماد على هذه التقنيات الحديثة، تنامي أيضًا تهديد "المخاطر الإلكترونية" التي أصبحت تشكل تحديًا كبيرًا أمام الأفراد والمؤسسات على حد سواء. هذه المخاطر تهدد الأمن الرقمي، وتستهدف المعلومات الشخصية، والبيانات الحساسة، وقد تؤدي إلى خسائر مالية هائلة أو تأثيرات نفسية واجتماعية عميقة. (Qaisi, 2023)

المخاطر الإلكترونية لا تقتصر على نوع واحد من الهجمات أو التهديدات، بل تتنوع بشكل كبير. من أبرز هذه المخاطر الهجمات السيبرانية التي يقوم بها القراصنة لسرقة البيانات أو تعطيل الأنظمة المعلوماتية. أحد أكثر الهجمات شيوعًا هي هجمات الفدية، حيث يقوم القراصنة بتشفير بيانات الضحايا ويطلبون فدية مالية مقابل فك التشفير. في عام 2020، على سبيل المثال، زادت هجمات الفدية بشكل كبير حيث تم استهداف العديد من المستشفيات في مختلف أنحاء العالم خلال جائحة كورونا. في أحد الحالات الشهيرة، تعرضت شبكة المستشفيات في ألمانيا لعملية قرصنة، مما أدى إلى تعطيل خدمات الرعاية الصحية وتأخير العمليات الجراحية، مما يبرز الخطورة التي قد تواجه القطاعات الحيوية نتيجة هذه الهجمات. (Mohammed, 2024)

على صعيد آخر، يشهد العالم أيضًا ازديادًا في عمليات "التصيد الاحتيالي" (Phishing)، والتي تعد من أكثر الأساليب شيوعًا لسرقة المعلومات الشخصية عبر الإنترنت. في هذه الهجمات، يقوم المهاجمون بإرسال رسائل إلكترونية أو رسائل نصية مزيفة تُخدع المستخدمين للنقر على روابط تؤدي إلى صفحات

وهمية، تهدف إلى سرقة كلمات المرور أو بيانات الحسابات البنكية. وفقًا لتقرير صادر عن شركة "سيمانتك" لعام 2021، تم رصد أكثر من 300 ألف حملة تصيد احتيالي في هذا العام فقط، وتسببت هذه الهجمات في خسائر ضخمة للمستخدمين حول العالم. (Redjem, 2022)

مخاطر أخرى تهدد الخصوصية الرقمية، مثل سرقة الهوية الإلكترونية. في هذه الحالة، يتم سرقة البيانات الشخصية للمستخدمين، مثل أرقام الضمان الاجتماعي، بيانات الحسابات البنكية، أو حتى سجلات طبية. هذه البيانات المسروقة يمكن أن تُستخدم لإجراء معاملات مالية غير قانونية، أو لاستغلال الضحايا في أعمال احتيالية. وفي دراسة حديثة، أشارت شركة "Experian" إلى أن أكثر من 15 مليون شخص في الولايات المتحدة وحدها وقعوا ضحية لسرقة الهوية في عام 2020، مما يشير إلى حجم المشكلة.

ولكن المخاطر الإلكترونية لا تقتصر على الأفراد فقط، بل تشكل تهديدًا بالغ الأهمية للمؤسسات والشركات الكبرى. الهجمات السيبرانية التي تستهدف الشركات قد تتسبب في خسائر مالية ضخمة، إذ تقدر تكلفة الهجمات الإلكترونية في العالم سنويًا بمليارات الدولارات. على سبيل المثال، شركة "مايكروسوفت" قامت بتقدير تكلفة الهجمات السيبرانية على الشركات في عام 2020 بحوالي 1 تريليون دولار أمريكي. من بين الأمثلة المشهورة، الهجوم الإلكتروني الذي استهدف شركة "Sony Pictures" في عام 2014، والذي أدى إلى تسريب بيانات حساسة للغاية، بما في ذلك الأفلام غير المعلنة ورسائل البريد الإلكتروني الخاصة بالموظفين التنفيذيين. هذا الهجوم تسبب في أضرار مالية ومعنوية كبيرة لشركة "Sony" وأثر بشكل سلبي على سمعتها. (Qaisi, 2023)

إلى جانب الأضرار الاقتصادية، هناك أيضًا أضرار نفسية واجتماعية تلحق بالضحايا الذين يتعرضون للمخاطر الإلكترونية. فعلى سبيل المثال، يُعتبر "التنمر الإلكتروني" أحد أسوأ أنواع المخاطر الاجتماعية التي قد يتعرض لها الأفراد في الفضاء الرقمي. هذا النوع من التنمر يشمل نشر رسائل تهديد أو تشويه سمعة الضحية عبر وسائل التواصل الاجتماعي، ويؤثر بشكل كبير على الصحة النفسية للأشخاص المعنيين، خاصة بين الشباب والمراهقين. وفقًا لدراسة قامت بها "مؤسسة Pew Research" عام 2020،

فإن ما يقرب من 59% من المراهقين الأمريكيين قد تعرضوا لشكله من التنمر الإلكتروني، مما يعكس انتشار هذا النوع من المخاطر. (Mohammed, 2024)

من جانب آخر، يُعتبر فقدان البيانات من أخطر التهديدات التي يواجهها الأفراد والشركات على حد سواء. إذ يمكن أن تؤدي الهجمات الإلكترونية إلى تدمير أو سرقة البيانات الهامة التي يصعب استعادتها، مثل البيانات المالية أو الطبية أو البحثية. في عام 2021، قامت شركة "IBM" بنشر تقرير يفيد بأن تكلفة تسريب البيانات في الشركات وصلت إلى حوالي 4.24 مليون دولار أمريكي في المتوسط لكل حادثة تسريب. هذه التكلفة تتضمن العواقب المالية المباشرة مثل غرامات المخالفات القانونية، بالإضافة إلى التأثيرات غير المباشرة مثل فقدان العملاء وتدهور السمعة. (Redjem, 2022)

ومع تزايد هذه المخاطر، أصبح من الضروري تعزيز الأمن السيبراني وتطوير الوعي الرقمي بين الأفراد والمؤسسات. يجب على الأفراد أخذ احتياطات قوية لحماية بياناتهم الشخصية، مثل استخدام كلمات مرور معقدة، وتفعيل خاصية التوثيق الثنائي، وتجنب فتح الروابط المشبوهة أو تحميل الملفات من مصادر غير موثوقة. كما أن على المؤسسات أن تضع استراتيجيات أمان متطورة لضمان حماية معلوماتها ومواردها من الهجمات المحتملة، بما في ذلك التدريب المستمر للموظفين على كيفية التعرف على المخاطر الإلكترونية. (Balishani, 2021)

أصبحت المخاطر الإلكترونية تهدد الجميع، من الأفراد العاديين إلى أكبر الشركات والحكومات، مما يستدعي تكاتف الجهود الدولية لوضع حلول فاعلة لمكافحة هذه التهديدات. من خلال التعاون بين الحكومات، شركات التقنية، والمنظمات غير الربحية، يمكن تعزيز الأمن السيبراني على المستوى العالمي. (Balishani, 2021)

1.1.2 مصادر المخاطر الإلكترونية

تتعرض المعلومات المحفوظة في الحواسيب والانظمة المستخدمة في حفظها للعديد من التهديدات التي قد يكون مصدرها من داخل المنشأة الموجودة فيها التقنية الحافظة لها، كما قد تتعرض للتهديدات من خارج هذه المنشأة. (Qaisi, 2023)

أولاً: الخطر الخارجي

يقوم بعض الاشخاص من خارج المنشأة بمحاولات لاختراق أمن الشبكات فيها، بهدف الدخول بشكل غير مصرح به للحصول على معلومات أو بيانات غير مصرح بها أو لغايات تعديل أو حذف هذه المعلومات أو البيانات، ويعتبر الخطر الناتج عن محاولاتهم هذه أقل خطورة عن غيره، ذلك أن القائمون على بناء وتركيب الشبكات يتوقعوا أن يكون هناك هجمات خارجية الأمر الذي يدفعهم الى بناء وتركيب شبكات على درجة عالية من الحرفية والدقة. (Mohammed, 2024)

ثانياً: الخطر الداخلي

يعتبر من أهم عوامل الحفاظ على المعلومات داخل المنشأة الافراد العاملون داخل هذه المنشأة، غير أن بعضهم يشكل خطراً حقيقياً على المعلومات وانظمتها ومراكزها، فهم المسؤولون عن برامج وانظمة التشغيل والصيانة والاستخدام. (Balishani, 2021)

ولعل هذا النوع من الخطر أشد فتكاً للمؤسسات لسهولة حدوثه وصعوبة الكشف عنه في كثير من الحالات، خصوصاً إذا كان المهاجم يمتلك صلاحية الولوج لنظام شبكات المعلومات، فلا يجد أي صعوبة في ذلك، بل يمكنه هذا الأمر من اخفاء ومحو أي آثار للدخول بسهولة ويسر، كما يعتبر هذا النوع من الخطر أشد خطورة عن غيره لكون المهاجم من الداخل بإمكانه إيجاد وتهيئة ثغرات في النظام الأمني للشبكات تمكن المهاجمون من الخارج باختراقه. (Redjem, 2022)

وتنقسم الافعال التي تقع من قبل العاملين داخل المنشأة الى افعال مقصودة وتكون عادة بتدبير وتخطيط تهدف الى اطلاع جهة غير مصرح لها على المعلومات أو نقل المعلومات أو تدميرها، كما قد تكون

افعال غير مقصودة ناتجة عن جهل أو ضعف في التدريب كترك الشاشات تعمل والمعلومات متاحة أو ترك كلمة السر أو ذكرها لأحد العاملين أو مسح المعلومات. (Balishani, 2021)

2.1.2 أهداف المخاطر الإلكترونية

تتوجه الاخطار الإلكترونية في بيئة المعلومات الى الأجهزة والتي تشمل كافة الادوات المادية كالشاشة والطابعة، كما قد تتوجه للبرامج وهي أوامر مرتبه في نسق معين لإنجاز الاعمال، وقد ينصب الخطر الإلكتروني على المعطيات والتي قد تكون في طور الادخال أو الاخراج أو التخزين أو التبادل بين النظم عبر الشبكات، وتشمل كافة البيانات المدخلة والمعلومات المستخرجة والبرامج المخزنة داخل النظام، كما قد ينصب الخطر على شبكات الاتصال التي تربط الاجهزة مع بعضها محلياً أو دولياً.

وتتعدد الاهداف التي يسعى المهاجم لتحقيقها من عملية القرصنة، نظراً لتعدد المعلومات في جميع نواحي الحياة وانتشارها، فيمكن أن تكون المعلومات تجارية، فيهدف المهاجم الى معرفة الاسرار المتعلقة بهذه التجارة أو الكشف عنها أو معرفة حسابات المؤسسة المستهدفة، كما قد تكون مالية فيهدف من خلال الهجوم للأضرار بالمؤسسة من خلال التلاعب بقيودها أو التلاعب بقيود المصارف، ويمكن أن يكون الهدف من القرصنة سياسي أو عسكري مثل الحصول على المخططات أو الملفات الحكومية أو العسكرية. (Balishani, 2021)

3.1.2 مجالات الخطر الإلكتروني

يعمل نظام المعلومات من خلال إدخال البيانات الى نظام الحاسوب حيث يتم معالجتها إلكترونياً لإنتاج المعلومات، فيتولى هذا النظام جمع ومعالجة البيانات وتخزينها وتحليلها وتجهيزها في سبيل تحقيق ذلك يتم استخدام تكنولوجيا المعلومات لإنجاز المهمة المطلوبة، ولذلك يمكن القول بأن نظام المعلومات يتكون من الحاسوب بكافة مكوناته البرامج، قاعدة البيانات شبكة الانترنت، والبيانات المخزنة. (Mohammed, 2024)

يسعى المهاجم من خلال نشاطه لاختراق هذا النظام بهدف الحصول على البيانات أو المعلومات المحفوظة فيه، لذلك ينصب هذا الاعتداء على الموارد أو المعلومات التي يهدف الشخص لحمايتها والمحافظة عليها لأهميتها، هذه الموارد والمعلومات هي ما يطلق عليها في علم أمن المعلومات بالأصول والتي تشمل الأجهزة الالكترونية والمعدات بالإضافة الى البرامج والمعلومات والبيانات المخزنة، ولذلك قسمت هذه الاصول الى عدة تقسيمات منها ما يسمى بأصول معلوماتية أي المحتوى الالكتروني المحفوظ أو المملوك للشخص أو المنشأة والتي تمثل البيانات وتعتبر من أهم الأصول وأكثرها تعرضاً لمحاولات الاعتداء، كما تشمل الاصول البرمجية وتشمل الأدوات البرمجية اللازمة لمعالجة البيانات، وعليه يمكن القول بأن الاعتداء يتم على هذه الأصول والتي تشمل المعلومات ونظم المعلومات. (Balishani, 2021)

4.1.2 صور المخاطر الإلكترونية

إن ازدياد كمية المعلومات التي تنتقل عبر شبكات المعلومات من مكان الى اخر حول العالم وإمكانية الوصول اليها من قبل الجميع ييسر وسهوله جعلها عرضة للمخاطر والتهديد والاختراق، اذ قد تكون هذه المعلومات ذات اهمية كبيره بحيث تكون الفيصل بين المكسب والخسارة سواء للمنشأة أم الفرد.

تتعدد تصنيفات المخاطر التي تتعرض لها المعلومات وذلك وفقاً للنظرة التي ينظر اليها هذه المخاطر، فاذا ما نظرنا اليها من حيث طبيعتها فيمكن تقسيمها الى مخاطر طبيعية ومخاطر بشرية ومخاطر بيئية، أما إذا نظرنا اليها من ناحية أمنية فان المختصون بالقضايا الأمنية عبر الشبكات والانترنت يقسمونها الى مخاطر تقنية ومخاطر غير تقنية، وكذلك يمكن تصنيفها من حيث مصدر هذا الخطر الى مخاطر داخلية ومخاطر خارجية. (Redjem, 2022)

يهدف الباحث من خلال استعراض بعض صور المخاطر التي تتعرض لها المعلومات التحديد مفهوم المخاطر الالكترونية والتي ستكون محلاً لدراسة الباحث، وقد تم تقسم هذه المخاطر الى ثلاثة صور تتمثل بالمخاطر الطبيعية والعامة والمخاطر الناتجة عن استخدام تكنولوجيا المعلومات.

– المخاطر الطبيعية.

تتعدد شبكات المعلومات وتنتشر في كافة بقاء الأرض، وتتأثر كغيرها من الأشياء بما يتعرض له كوكبنا من كوارث طبيعية والتي قد تقع دون سابق انذار ودون تدخل من البشر فالشبكات وبنيتها عرضة لخطر الزلازل والبراكين والانفجارات والحرائق وغيرها من الكوارث الطبيعية والتي تؤدي الى تلف الاجهزة وضياع المعلومات والبيانات المحفوظة فيها. (Mohammed, 2024)

– ثانياً: المخاطر العامة

تتم عملية إرسال أو تلقي أو مشاركة المعلومات والاتصال من خلال ربط حاسوبين أو أكثر بحيث يتم إنشاء شبكه تتم من خلالها هذه العمليات، لذلك يعتبر الحاسوب وبنك المعلومات من أبرز وسائل تخزين ومعالجة واسترجاع المعلومات، وتعد عملية تصميم الشبكات والانظمة واستخدام انواع جيده من البرامج سبباً مباشراً في نجاح عملية انتقال المعلومات والبيانات والمحافظة عليها من أي ضياع أو عبث، لذلك فإن وجود بعض الاخطاء أو الغيوب الفنية في التصميم أو الانظمة أو البرامج التي تعمل بها الشبكات يعتبر من قبيل الاخطار العامة التي تهدد المعلومات المحفوظة فيها. (Balishani, 2021)

تعمل الحاسبات من خلال امدادها بالطاقة الكهربائية، فيعتبر انقطاع تزويد الحاسبات بالطاقة الكهربائية من قبيل الاخطار العامة التي تتعرض لها الحاسبات والمعلومات المحفوظة فيها، فانقطاع التيار الكهربائي قد يؤدي الى تلف هذه الأجهزة أو ضياع وفقدان المعلومات أو تلفها كذلك الحال فيما يتعلق بانقطاع خدمة الاتصال أو الانترنت التي قد تؤدي الى تلف أو ضياع المعلومات.

5.1.2 أهمية المخاطر الإلكترونية في العصر الرقمي

في العصر الرقمي الذي نعيش فيه اليوم، أصبحت التكنولوجيا عنصراً أساسياً في حياتنا اليومية، حيث غيرت الطريقة التي نتواصل بها، ونعمل، ونتعلم، ونستهلك الخدمات. أصبح الإنترنت شبكة حيوية تربط جميع جوانب حياتنا، من التواصل الاجتماعي إلى الأنشطة التجارية، ومن التعليم إلى الرعاية الصحية. ومع هذه الثورة الرقمية التي تمثل تقدماً كبيراً في العديد من المجالات، تظهر في المقابل مخاطر

إلكترونية تهدد أمن الأفراد والمؤسسات على حد سواء. هذه المخاطر لا تقتصر فقط على التهديدات التقليدية مثل الفيروسات، بل تشمل أيضًا هجمات معقدة ومؤذية قد تؤدي إلى فقدان البيانات، سرقة الهوية، وتهديدات أخرى قد تؤثر على الأمن الشخصي والاجتماعي. (Qaisi, 2023)

إن أهمية المخاطر الإلكترونية في العصر الرقمي ليست مجرد مسألة تهديدات أمنية فردية، بل إنها تؤثر بشكل أوسع على المجتمع ككل. فعلى المستوى الشخصي، أصبح الأفراد أكثر عرضة للتهديدات مثل سرقة البيانات الشخصية، الاحتيال الإلكتروني، والتصيد الاحتيالي، حيث أن المعلومات الحساسة مثل كلمات المرور، التفاصيل البنكية، والبيانات الشخصية الأخرى أصبحت مستهدفة من قبل قراصنة الإنترنت. هذه المخاطر تؤثر في مستوى ثقة الأفراد في استخدام التكنولوجيا، وقد تقود البعض إلى اتخاذ خطوات احترازية غير ضرورية أو حتى التوقف عن استخدام الإنترنت بالكامل خوفًا على خصوصيتهم.

على المستوى المؤسسي، تشكل المخاطر الإلكترونية تهديدًا أكبر نظرًا لحجم البيانات والأنظمة التي تحتاج إلى حماية. فقد تواجه الشركات والمنظمات هجمات واسعة النطاق مثل البرمجيات الخبيثة، برامج الفدية، والهجمات الموزعة التي تستهدف تعطيل أو تدمير البنية التحتية الرقمية. الهجمات السيبرانية قد تؤدي إلى فقدان بيانات حساسة، مما يتسبب في خسائر مالية ضخمة، وتضرر السمعة التجارية، وانخفاض ثقة العملاء. كما أن هذه الهجمات يمكن أن تؤثر على استمرارية العمليات التجارية، خصوصًا في المؤسسات التي تعتمد بشكل كبير على الأنظمة الرقمية في تقديم خدماتها. (Balishani, 2021)

المخاطر الإلكترونية تمتد أيضًا إلى المؤسسات الحكومية، حيث تستهدف الهجمات الأمنية بيانات الدولة الحساسة، بما في ذلك البيانات العسكرية، الدبلوماسية، والمعلومات الاقتصادية الهامة. في بعض الحالات، قد تتعرض البلدان لخطر فقدان السيطرة على أنظمتها الرقمية أو حتى تعطيل البنية التحتية الحيوية مثل شبكات الكهرباء والمياه. الهجمات السيبرانية على مستوى الحكومات تشكل تهديدًا ليس فقط للأمن الوطني، بل للأمن العالمي أيضًا، حيث يمكن أن تؤدي إلى زعزعة الاستقرار في مناطق بأكملها إذا كانت الهجمات ذات تأثير عميق على الحكومة والشعب.

ومع تزايد حجم المخاطر الإلكترونية وتعقيدها، أصبحت الحاجة إلى تعزيز الأمن السيبراني أمرًا ضروريًا. تزايدت الدعوات من قبل الخبراء في الأمن الرقمي إلى ضرورة اتخاذ تدابير أكثر فاعلية للوقاية من الهجمات الإلكترونية، بما في ذلك تطبيق سياسات أمنية صارمة على مستوى الأفراد والشركات، وتوفير برامج توعية للمستخدمين حول كيفية التصدي للمخاطر الإلكترونية. في هذا السياق، تعتبر الحكومات والمؤسسات التكنولوجية بحاجة ماسة للتعاون من أجل تطوير استراتيجيات شاملة للأمن السيبراني لمكافحة التهديدات المتزايدة. (Balishani, 2021)

إذن، في هذا العصر الرقمي المترابط والمتطور بشكل مستمر، يصبح من الضروري أن نفهم أهمية المخاطر الإلكترونية وكيفية التصدي لها بشكل فعال. إن تعزيز وعي الأفراد والمجتمعات حول هذه المخاطر، وتبني أساليب وقائية متقدمة، قد يساهم في بناء بيئة رقمية آمنة تمكننا من الاستفادة من فوائد التكنولوجيا مع تقليل المخاطر التي قد تواجهها. إن الأمن الإلكتروني لا يعد رفاهية أو خيارًا، بل ضرورة حيوية لضمان استقرار الأفراد والمجتمعات والمؤسسات في عالم رقمي يتسم بالتطور المستمر والتهديدات المتزايدة.

6.1.2 أنواع المخاطر الإلكترونية

في ظل التوسع الكبير في استخدام التكنولوجيا الحديثة، أصبح الإنترنت جزءًا أساسيًا من حياتنا اليومية، حيث يتيح لنا التواصل والعمل والتعلم والتسوق، بل وحتى إجراء المعاملات المالية. لكن مع هذه الفوائد العديدة، تأتي أيضًا مجموعة من المخاطر الإلكترونية التي تهدد الأفراد والمجتمعات والمؤسسات على حد سواء. تتنوع هذه المخاطر بشكل كبير، وتشمل العديد من الأنواع التي تختلف في درجة تأثيرها، من تهديدات بسيطة قد تسبب في إزعاج إلى هجمات معقدة قد تؤدي إلى خسائر فادحة. ومن هنا، فإن فهم هذه الأنواع المتنوعة من المخاطر الإلكترونية يعد أمرًا بالغ الأهمية من أجل اتخاذ التدابير الوقائية اللازمة. (Redjem, 2022)

من أبرز أنواع المخاطر الإلكترونية، تأتي البرمجيات الخبيثة التي تشمل الفيروسات، الديدان، وبرامج الفدية. هذه البرمجيات تتمثل في أكواد ضارة تهدف إلى اختراق الأنظمة وإلحاق الضرر بها. الفيروسات على سبيل المثال، تعد من أشهر البرمجيات الخبيثة، حيث تقوم بتكرار نفسها داخل الملفات

والنظام، مما يؤدي إلى تدمير البيانات أو تعطيل الأنظمة. أما الديدان، فهي نوع آخر من البرمجيات التي تنتقل عبر الشبكات، مما يسمح لها بالانتشار بسرعة بين أجهزة الحاسوب. وعلى الرغم من أن البرمجيات الخبيثة قد تكون غير مرئية في بعض الأحيان، إلا أنها غالبًا ما تؤدي إلى تعطيل العمل داخل الأجهزة أو سرقة البيانات. وفي السنوات الأخيرة، شهدنا انتشار برامج الفدية التي تشفر الملفات على جهاز الضحية وتطلب فدية مالية مقابل فك التشفير، وهي من أخطر التهديدات التي تواجه الأفراد والشركات على حد سواء.

(Mohammed, 2024)

بالإضافة إلى ذلك، تمثل الهجمات السيبرانية أحد الأنواع الأكثر شيوعًا وأكثر تعقيدًا من المخاطر الإلكترونية. وهذه الهجمات قد تشمل مجموعة واسعة من الأنشطة غير القانونية مثل القرصنة واختراق الأنظمة لسرقة البيانات أو تعطيلها. القراصنة الإلكترونيون قد يستهدفون الشركات الكبرى للحصول على معلومات حساسة أو أموال، أو حتى قد يستهدفون الأفراد بسرقة معلوماتهم المالية أو الشخصية. من أبرز أنواع الهجمات السيبرانية التي تسببت في مشاكل كبيرة في السنوات الأخيرة هي هجمات حجب الخدمة (DDoS)، التي تستهدف إغراق الخوادم بالمزيد من البيانات مما يؤدي إلى تعطل المواقع والخدمات عبر الإنترنت. كما أن هناك الهجمات المتقدمة المستمرة (APT) التي تستهدف المؤسسات الكبرى والشركات الحكومية، حيث يكون الهجوم محكمًا وموجهًا بدقة بهدف جمع المعلومات الحساسة لفترة طويلة.

(Balishani, 2021)

لا تقتصر المخاطر الإلكترونية على تهديدات البرمجيات والهجمات فقط، بل تمتد أيضًا إلى الاحتيال الإلكتروني. وتعد هجمات التصيد الاحتيالي (Phishing) من أبرز الأساليب التي يستخدمها المهاجمون لسرقة المعلومات الحساسة. في هذه الهجمات، يقوم المهاجمون بإرسال رسائل مزيفة تشبه رسائل من مؤسسات موثوقة مثل البنوك أو خدمات الإنترنت، بهدف خداع المستخدمين للكشف عن كلمات المرور أو المعلومات الشخصية. ومن جهة أخرى، يظل الاحتيال المالي عبر الإنترنت من أخطر التهديدات، حيث يتم استغلال ثغرات في أنظمة الدفع الإلكتروني أو مواقع التجارة الإلكترونية لإجراء

معاملات غير قانونية قد تؤدي إلى خسائر مالية ضخمة للأفراد والشركات. (Redjem, 2022)

إلى جانب هذه الأنواع، يعتبر التنمر الإلكتروني من أبرز المخاطر الاجتماعية التي تنشأ نتيجة لاستخدام الإنترنت. هذا النوع من المخاطر يهدد الأفراد بشكل خاص، سواء كانوا في سن المراهقة أو حتى في مراحل متقدمة من العمر. التنمر الإلكتروني يتمثل في المضايقات أو التهديدات التي تتم عبر الإنترنت، سواء من خلال الرسائل المسيئة أو نشر معلومات مغلوطة بهدف التشويه أو الإهانة. وهو قد يترك آثارًا نفسية عميقة على الضحايا، وقد يؤدي إلى حالات من الاكتئاب أو القلق الشديد، مما يعكس أهمية الوعي المجتمعي في مواجهة هذا النوع من المخاطر.

أخيرًا، لا يمكن إغفال المخاطر المتعلقة بالخصوصية والبيانات الشخصية في العصر الرقمي. في ظل الانتشار الواسع للأجهزة الذكية والتطبيقات التي تجمع وتخزن البيانات الشخصية، أصبح من السهل على المهاجمين الوصول إلى معلومات حساسة مثل تفاصيل الحسابات البنكية، عناوين البريد الإلكتروني، وأرقام الهواتف. قد تكون هذه المعلومات معرضة للسرقة عبر تقنيات مثل الاستغلال غير المصرح به أو تسريب البيانات، حيث يضع المهاجمون أيديهم على البيانات الشخصية بهدف بيعها أو استخدامها في أغراض غير قانونية. في بعض الحالات، قد يتم استغلال هذه البيانات في الاحتيال الإلكتروني أو سرقة الهوية، مما يسبب ضررًا كبيرًا للأفراد في حياتهم الشخصية والمهنية. (Redjem, 2022)

بناءً على ذلك، تكمن أهمية الوعي بتنوع المخاطر الإلكترونية في فهم كيفية التفاعل معها بشكل آمن. لا تقتصر هذه المخاطر على أفراد بعينهم أو مؤسسات محددة، بل تؤثر في جميع مستخدمي التكنولوجيا، مما يتطلب اتخاذ خطوات وقائية على جميع المستويات. من خلال التعليم والتدريب المناسبين، يمكن تقليل مخاطر التعرض لهذه الأنواع المختلفة من التهديدات، مما يساعد في خلق بيئة إلكترونية أكثر أمانًا وفاعلية.

7.1.2 الوقاية والحماية من المخاطر الإلكترونية

في العصر الرقمي الذي نعيشه اليوم، أصبحت المخاطر الإلكترونية تهدد بشكل متزايد الأفراد والمؤسسات على حد سواء. من سرقة الهوية إلى الهجمات السيبرانية المعقدة، تتنوع التهديدات الإلكترونية التي قد تؤثر على الأمان الشخصي وتضر بالبيانات الحساسة. ولكن في ظل هذه المخاطر، توجد

استراتيجيات وأدوات وقائية يمكن أن تساعد في تقليل احتمالية التعرض لهذه الهجمات وحماية المعلومات والأنظمة. يعتمد الأمان الرقمي على اتخاذ تدابير وقائية متعددة تضمن الحماية من هذه التهديدات، والتي تشمل استراتيجيات الأمان الشخصي، أدوات وبرمجيات الأمان، بالإضافة إلى التثقيف الرقمي المستمر. (Balishani, 2021)

من أبرز استراتيجيات الأمان الشخصي التي يجب على كل فرد اتباعها هي استخدام كلمات مرور قوية. لا يقتصر الأمر على اختيار كلمات مرور بسيطة يمكن تخمينها بسهولة، بل يجب أن تكون معقدة، تحتوي على مزيج من الحروف الكبيرة والصغيرة، الأرقام، والرموز الخاصة. يمكن لتغيير كلمات المرور بشكل دوري واستخدام كلمات مرور فريدة لكل حساب أن يقلل بشكل كبير من احتمالية تعرض الأفراد للاختراقات. بجانب ذلك، تفعيل التوثيق الثنائي يعد خطوة أساسية لحماية الحسابات الشخصية. هذه العملية تضيف طبقة إضافية من الأمان عن طريق طلب رمز تحقق يتم إرساله إلى هاتفك المحمول أو عبر تطبيق خاص بعد إدخال كلمة المرور. حتى إذا كانت كلمة المرور قد تعرضت للاختراق، فإن هذه الطبقة الإضافية تجعل من الصعب الوصول إلى الحسابات. (Mohammed, 2024)

من الأمور المهمة أيضاً في الوقاية من المخاطر الإلكترونية هو الحذر عند التعامل مع البريد الإلكتروني والمواقع الإلكترونية. كثير من الهجمات الإلكترونية تبدأ برسائل تصيد احتيالي تحمل روابط أو مرفقات ضارة. لذا، يجب أن يكون المستخدم حذراً للغاية في فتح الرسائل من مصادر غير معروفة أو مشبوهة. كما أن زيارة المواقع الإلكترونية المشبوهة أو الغير آمنة يمكن أن تعرض الأجهزة للخطر، لذلك من المهم التأكد من أن الموقع يستخدم بروتوكول HTTPS وتحقق من مصداقية المواقع قبل إدخال أي بيانات شخصية.

أما على مستوى الأدوات التقنية، فلا غنى عن برامج مكافحة الفيروسات التي تعد خط الدفاع الأول ضد البرمجيات الخبيثة مثل الفيروسات، الديدان، وبرامج الفدية. هذه البرمجيات تقوم بالكشف عن التهديدات قبل أن تتمكن من إلحاق الضرر بالنظام أو سرقة البيانات. لكن استخدام برامج مكافحة الفيروسات وحدها لا يكفي، حيث يجب أيضاً تثبيت جدران الحماية (Firewall)، التي تعمل على مراقبة

حركة مرور البيانات بين جهازك والإنترنت، مما يحد من إمكانية وصول المهاجمين إلى جهازك من خلال شبكات غير آمنة. إن جدران الحماية يمكن أن تمنع العديد من محاولات الاختراق وتحد من تهديدات الشبكات الخارجية.

كذلك، أدوات مكافحة التصيد تعتبر من الأدوات الفعالة في الكشف عن رسائل البريد الإلكتروني والمواقع المزيفة التي تهدف إلى خداع المستخدمين لاستخراج معلوماتهم الشخصية أو المالية. تتضمن هذه الأدوات تقنيات للكشف التلقائي عن الروابط المشبوهة أو تصفية الرسائل التي تحتوي على محاولات تصيد، مما يساهم في حماية المستخدمين من الوقوع في فخ الاحتيال الإلكتروني.

ولكن لا تقتصر الوقاية من المخاطر الإلكترونية على الأدوات التقنية فقط، بل هي عملية يجب أن تكون مدعومة بـ التثقيف الرقمي والوعي الأمني. فالتوعية حول الأمان السيبراني تعتبر من الركائز الأساسية في الحد من المخاطر الإلكترونية. من خلال تعلم مبادئ الأمان الرقمي، مثل كيفية التعامل مع كلمات المرور، كيفية التحقق من صحة الرسائل الإلكترونية، وكيفية تصفح الإنترنت بأمان، يمكن للأفراد أن يصبحوا أكثر وعياً بالمخاطر المحيطة بهم. هذا التثقيف لا يقتصر على الأفراد فقط، بل يجب أن يمتد ليشمل تدريب الموظفين في المؤسسات أيضاً. المؤسسات التي تعتمد على الأنظمة الرقمية تحتاج إلى تدريب مستمر للموظفين حول كيفية التعرف على الهجمات السيبرانية مثل التصيد الاحتيالي، وكيفية التصرف في حال حدوث أي تهديد إلكتروني. هذا التدريب يساهم بشكل كبير في تقليل فرص حدوث هجمات ناجحة ويعزز من قدرة الموظفين على حماية البيانات التي تديرها المؤسسات. (Balishani, 2021)

من خلال تنفيذ هذه الاستراتيجيات الوقائية واستخدام الأدوات المناسبة، يمكن تقليل المخاطر الإلكترونية بشكل ملحوظ. في النهاية، لا يمكن الاعتماد فقط على التقنيات المتطورة، بل يجب أن يكون هناك وعي دائم حول التهديدات الإلكترونية وكيفية التعامل معها، مما يضمن بيئة رقمية أكثر أماناً لكل من الأفراد والمؤسسات. (Mohammed, 2024)

المبحث الثاني: أداء المنظمة

المقدمة

إن الظروف الحالية تجعل المنظمات تواجه العديد من الضغوطات الناتجة عن التغيرات السريعة التي تشهدها بيئة الأعمال المعاصرة، هذا ما جعلها تسعى وبصورة مستمرة نحو التطور، والإبداع والتجديد والتحسين باعتباره الطريق الوحيد لاستمرارها ونموها، وبهذا إن تحسين الأداء وتطوير وتجديد المنظمات لم يعد أمراً اختيارياً، ولكنه أصبح شرطاً جوهرياً لإمكان البقاء والاستمرارية وعدم الاندثار في هذا المحيط التنافسي الذي يعد التغيير فيه هو الثابت الوحيد، ويعتمد في قدراتها على التقييم الفعال لأدائها وفي تحديد الاستراتيجيات التي تمكنها من التحسين في قراراتها وبلوغ أهدافها. (Barbary, 2020)

لذا كان الاهتمام في الآونة الأخيرة بقضية الأداء من منظور كلي شامل، يستهدف في الأساس تكوين وتدعيم القدرات التنافسية، وأصبحت المنظمة الآن تهدف لتحقيق أحسن أداء في ميدان نشاطها.

وفي هذا الإطار نجد أن المنظمات قد استخدمت العديد من الأدوات و أنظمة قياس وتقييم الأداء بهدف جمع المعلومات الصحيحة لدعم عملية اتخاذ القرارات وتحسين أدائها، إلا أنه مع ذلك لا يزال قياس الأداء ووضع الاستراتيجيات الفعالة يمثل تحدياً مستمراً بالنسبة للمنظمات بسبب الطبيعة المعقدة التي تتميز المنظمات عن غيرها من جهة و عدد المتغيرات المتزايد المؤثرة فيها من جهة أخرى. (الجري، 2019)

1.2.2 أداء المنظمة: مفاهيم أساسية:

يعبر أغلب الباحثين والكتاب عن الأداء من خلال مدى النجاح الذي تحرزه المنظمة في تحقيق أهدافها وبالرغم من ذلك فإن هناك تباين بين العديد منهم في دراساتهم بالأداء، حيث لم يتم التوصل إلى إجماع حول مفهوم محدد للأداء، وذلك لاختلاف المعايير والمقاييس المعتمدة في دراسة الأداء وقياسه، وكذا لتنوع أهداف واتجاهات الباحثين في دراستهم للأداء، ولذا سيتناول هذا المبحث مفاهيم الأداء، تصنيفاته ومستوياته وأخيراً محدّداته ومعوّقاته.

أولاً: مفهوم أداء المنظمة

يعد الأداء مفهوماً جوهرياً بالنسبة للمنظمات، وله العديد من المفاهيم المتعددة المعاني، وقد اختلف الباحثون في طرح مفهومه حسب إختلاف الخلفيات الفكرية فمنهم من يرى أن الأداء هو المخرجات أو الأهداف التي يسعى النظام إلى تحقيقها لذا فهو مفهوم يعكس كلا من الأهداف والوسائل اللازمة لتحقيقه، وحيث يرى البعض أن السبب يعود الى إختلاف طبيعة عمل المنظمات وأهدافها والجهات التي تقيسها، ويرتبط مفهوم الاداء بسلوك الفرد والمنظمة، ويحتل مكانة خاصة داخل أي مؤسسة باعتبارها الناتج النهائي لمحصلة جميع الأنشطة فيها. (الجري، 2019)

أولاً: الاداء في اللغة:

الاداء اسم مصدر للفعل (أدى)، ومصدره التأدية، ومعناه على ما صرح به بعض أهل اللغة: القضاء يقال: أدى فلان دينه تأدية، أي قضاها كما ورد في الصحاح، وقيل:

بل أصله إيصال الشيء الى الشيء أو وصله إليه من تلقاء نفسه، وجمع بعض اللغويين بين معني الإيصال والقضاء، ففي القاموس: أداء تأدية: أوصله وقضاه، والاسم: الاداء، وفي مجمع البحرين (أدا) في قوله تعالى: "وأداءً إليه باحسان" سورة البقرة (الآية: 178) أي إيصال إليه وقضاء ومنه وأدى دينه، و أدى الأمانة إلى أهلها)، أي أوصلها والاسم الأداء.

ونشير إلى أن الأداء لغة يقابل اللفظة اللاتينية Performare التي تعني إعطاء كلية الشكل لشيء ما، والتي اشتقت منها اللفظة الإنجليزية Performance التي تعني إنجاز العمل أو الكيفية التي يبلغ بها التنظيم أهدافه وهو نفس المعنى الذي ذهب إليه قاموس Petit Larousse ولكن اللغة الانجليزية هي التي اعطت له معنى واضح ومحدد للقيام بفعل يساعد على الوصول الى الاهداف المسطرة. (Barbary, 2020)

ثانياً: الاداء في الاصطلاح

فقد وضع Miller & Bromiley أن الأداء محصلة قدرة المنظمة في استغلال مواردها وتوجيهها نحو تحقيق الأهداف المنشودة، فالأداء هو انعكاس لكيفية استخدام المنظمة لمواردها المادية والبشرية، واستغلالها بالصورة التي تجعلها قادرة على تحقيق أهدافها. (الجري، 2019)

وعرفه Wheelen & Hunger على أنه تركيز أهداف البقاء والتكيف والنمو وهي أهداف طويلة المدى بالنسبة للمنظمة.

وأضاف Daft على أنه قدرة الشركة على تحقيق أهدافها عن طريق استخدام الموارد المتاحة بطريقة كفؤة وفعالة، كما وصفه البرنامج الوطني للجودة بأنه تعبير عن المخرجات التي يتم الحصول عليها من المنتجات والعمليات.

ويُعرف الأداء أيضاً بأنه "درجة النجاح التي تحققها المنظمة في إنجاز الأهداف المحققة مسبقاً، وكما يعرف على أنه درجة بلوغ الأفراد أو الفرق أو المنظمة للأهداف المخططة بكفاءة وفعالية.

ومن خلال استعراض المفاهيم والتعاريف السابقة للأداء لاحظ الباحث عدة نقاط لا يخلوا أي تعريف منها: (Barbary, 2020)

1. أن الأداء هو حاصل تفاعل عنصرين أساسيين هما الطريقة في استعمال موارد المنظمة، ونقص ذلك عامل الكفاءة، والنتائج المحققة من ذلك الاستخدام، ونعني بذلك عامل الفعالية.
2. أن أهمية هذا المفهوم بالنسبة للمنظمات ومؤسسات الأعمال تكمن في أن الأداء يستعمل للحكم على هذه المنظمات والمؤسسات من حيث قدرتها على تحقيق أهدافها.
3. أن مفهوم الأداء يقترن بمصطلحين هامين في الإدارة هما الكفاءة والفعالية.
4. أن الأداء هو مدى قدرة الفرد أو الفريق أو المنظمة على تحقيق أهدافها على المدى البعيد.
5. أن القدرة على تحقيق الأهداف تتم من خلال ترشيدها في استغلال وتوظيف مختلف مواردها المادية والبشرية.

6. الأخذ بعين الاعتبار تأثيرات البيئة الداخلية والخارجية لأنشطتها.

7. أن الكفاءة تعمل على التقليل أو التخفيض في رأس المال العمل المواد الأولية المعلومات بينما تعمل

الفعالية على زيادة الإنتاج الربح القيمة المضافة، رقم الأعمال ويعمل الأداء على استخدام كل من

الكفاءة والفعالية من أجل تحقيق النمو والاستمرارية.

ولذلك سنورد تعريف هذين المصطلحين وهما كالآتي:

الفعالية هي محصلة تفاعل مكونات الأداء الكلي للمنظمة بما تحتويه من أنشطة فنية وإدارية وما

يؤثر فيه من متغيرات داخلية أو خارجية، أو هي زيادة معدل العائد على الاستثمار بكافة الطرق، أو هي

القدرة على البقاء والاستمرار والتحكم في البيئة، أو هي قدرة المنظمة على تحقيق أهدافها التشغيلية.

(الجري، 2019)

2.2.2 ثانياً: تصنيفات الأداء ومستوياته

1. تصنيفات الأداء

توجد عدة تصنيفات للأداء وهذا يعود كما تم الإشارة إليه سابقاً لاختلاف اتجاهات الباحثين،

ويمكن تصنيف الأداء استناداً إلى عدة معايير، وبما أن الأداء من حيث المفهوم يرتبط إلى حد بعيد بالأهداف

فإنه يمكن نقل المعايير المعتمدة في تصنيف هذه الأخيرة واستعمالها في تصنيف الأداء، ومن أهم هذه

المعايير، معيار مصدر الأداء، معيار الشمولية والمعيار الوظيفي. (Barbary, 2020)

• تصنيفات الأداء حسب معيار المصدر

وفقاً لهذا المعيار يمكن تقسيم أداء المنظمة إلى أداء داخلي وخارجي:

○ الأداء الداخلي وينتج من تفاعل مختلف أداءات الأنظمة الفرعية للمنظمة أي مختلف الأداء الجزئية

متمثلة في الأداء البشري أي الموارد البشرية في المنظمة، والأداء التقني الذي يتعلق بجانب

الاستثمارات، والأداء المالي الخاص بالإمكانيات المالية المستعملة. وبمعنى آخر الأداء الداخلي يتمثل في قدرة المنظمة على استعمال مواردها البشرية والتقنية والمالية بشكل فعال.

○ الأداء الخارجي: ويعرف بالأداء الناتج عن التغيرات التي تحدث في البيئة المحيطة الخارجية للمنظمة، وحتى يتحقق الأداء لابد للمنظمة من التنبؤ بالتغيرات التي تحدث في البيئة المحيطة بها والاستجابة السريعة لها، فهذه التغيرات الخارجية تؤدي إلى تغير في مسار المنظمة، فنجاعها أو فشلها يتحدد من خلال قدرتها على الملاءمة مع بيئتها الخارجية. ويظهر هذا الأداء عند ارتفاع رقم الأعمال نتيجة زيادة حجم المبيعات أو الارتفاع سعر البيع أو خروج أحد المنافسين، أو ارتفاع القيمة المضافة مقارنة بالسنة الماضية نتيجة لانخفاض أسعار المواد واللوازم والخدمات، فان هذه التغيرات تؤثر في الأداء إما بالإيجاب أو بالسلب وبالتالي يجب على المنظمة قياس وتحليل هذا الأداء، لأنه يمكن أن يشكل تهديدا لها فهي لا تتحكم فيه كما هو الحال بالنسبة للأداء الداخلي.

ومن خلال هذين النوعين من الأداء الداخلي والخارجي يتضح أن أداء المنظمة ينتج من خلال استغلالها لمختلف مواردها المتاحة (نقاط القوة) بكفاءة وفعالية من جهة واستغلال الفرص المتاحة من الخارج من جهة أخرى.

● تصنيفات الأداء حسب معيار الشمولية

يمكن تقسيم الأداء حسب هذا المعيار إلى:

○ الأداء الكلي: وهو الذي يتجسد بالإنجازات التي ساهمت جميع العناصر والوظائف والأنظمة الفرعية للمنظمة في تحقيقها، ولا يمكن أن ننسب إنجازها إلى أي عنصر أو احد فروعها دون مساهمة باقي العناصر.

○ الأداء الجزئي: وهو الذي يتحقق على مستوى الأنظمة الفرعية للمنظمة وينقسم بدوره إلى عدة أنواع تختلف باختلاف المعيار المعتمد لتقسيم عناصر المنظمة، حيث يمكن أن ينقسم حسب المعيار الوظيفي إلى أداء وظيفة المالية أداء وظيفة الأفراد، أداء وظيفة التمويل أداء وظيفة الإنتاج وأداء وظيفة التسويق.

وفي إطار هذا النوعين يرى الباحث عن مدى وكيفية بلوغ وتحقيق المنظمة أهدافها من خلال تفاعل وتكامل أداء أنظمتها الفرعية كما نجد أن دراسة الأداء الشامل للمنظمة يحتم أيضا دراسة الأداء على مستوى مختلف وظائفها وبذلك تتحقق أهدافها الشاملة كالأستمرارية، الشمولية الأرباح النمو بأدنى التكاليف الممكنة، وأحسن وافضل جودة. (الجرفي، 2019)

• تصنيفات الأداء حسب المعيار الوظيفي

حسب هذا المعيار يقسم الأداء إلى أداء الوظائف الأساسية وهي الإنتاج المالية التسويق، والموارد البشرية ويتم تقسيم الأداء إلى:

1. أداء الوظيفة المالية ويتمثل في قدرة المنظمة على تحقيق التوازن المالي، وبناء هيكل مالي فعال بالإضافة إلى تحقيق المردودية وتعظيم العائد على الاستثمار باعتباره أحد أهم أهداف المنظمة، لذا فإن البعد المالي للأداء الكلي للمنظمة يتحقق من خلال تحقيق المردودية وتعظيمها، مما طرح فكرة ربط المكافآت الممنوحة للإداريين في المنظمة بحجم المردودية التي ساهموا في تحقيقها، أي تكون متناسبة طرديا معها وهذا من شأنه أن يرسخ لدى الإداريين فكرة أنهم مستثمرون (مساهمون في المنظمة أي مساهمون فيها وليسوا إداريين فقط، وبالتالي يعملون على زيادة مردوديتها أكثر فأكثر.
2. أداء وظيفة التسويق: يتحدد هذا الأداء من خلال مجموعة من المؤشرات المتعلقة بوظيفة التسويق منها تحسين حجم المبيعات، رفع قيمة الحصة السوقية، تحقيق رضا العملاء، شهرة العلامة التجارية وبناء سمعة طيبة لدى المستهلكين ... إلخ.

إن حقيقة أداء الوظيفة التسويقية تعد من التحديات الكبرى في المنظمة إذ تطرح مشكلة قدرة تقييم الرضى، ومقدار تأثير الحملات التسويقية على الزبائن أو العملاء، هذا ما يفسر نسبة الدوران العالية للعاملين في هذه المنظمة وذلك راجع لصعوبة تقييم أدائهم مما ينشعب عنه في كثير من الأحيان خلافات كبيرة بين العاملين، تفسر غالبا بالنسبة المرتفعة للاستقلالات.

3. أداء وظيفة الإنتاج: يتحقق عندما تحقق المنظمة إنتاجية مرتفعة مقارنة بالمنظمات الأخرى من خلال إنتاج منتجات بجودة عالية وبتكاليف أقل تسمح لها بالمنافسة، بالإضافة إلى تخفيض التعطيلات الناتجة عن توقف الآلات أو التأخر في تلبية الطلبات، ويكون ذلك بالتحكم بطريقة العمل بيئة العمل تكاليف الإنتاج، كفاءة العمال، التحكم بالوقت والإنتاج، المراقبة على الآلات معدل التأخر. (الجري، 2019)

4. أداء وظيفة الأفراد (الموارد البشرية) وتعد وظيفة الموارد البشرية من أهم وأصعب الوظائف في تحديد مفهوم الأداء، إذ أن العنصر البشري عنصر متغير يصعب تحديد كفاءته وفعاليته بشكل واضح، وقد يستعين القائمون على تحديد أداء العنصر البشري المؤشرات المستوى العلمي والمهارة الفنية إلا أنها تبقى جد قاصرة عن إعطاء التقييم الكامل فالجانب النفسي كالعامل تحت الضغط والتوتر عوامل لا يمكن إخضاعها للدراسة أو الوصف الذي يمكن معه تحديد الأسباب بشكل دقيق. (Barbary, 2020)

● تصنيفات الأداء حسب معيار الطبيعة:

يندرج تحت هذا المعيار التصنيفات الآتية:

- الأداء الاقتصادي: يتم قياس الأداء الاقتصادي باستخدام الربحية أو المردودية بأنواعها المختلفة ومن أهم الأدوات المستخدمة التحليل المالي على الرغم من أن التشخيص الاقتصادي لابد أن يتماشى جنباً إلى جنب مع التشخيص المالي للوصول إلى نتائج هامة حول الأداء الاقتصادي.
- الأداء الاجتماعي: يعد الأداء الاجتماعي لأي منظمة أساساً لتحقيق المسؤولية الاجتماعية، ويتميز هذا النوع بصعوبة إيجاد المقاييس الكمية، لتحديد مدى مساهمة المنظمة في المجالات الاجتماعية التي تربط بينها وبين الجهات التي تتأثر بها.
- الأداء التكنولوجي: تعد التكنولوجيا من بين مصادر الأفضلية التنافسية والتميز في الأداء، لذا فإن الأداء التكنولوجي يرتبط إلى حد كبير بامتلاكها ومدى تطويرها وتحسينها مع المستجدات، لذلك تكون الأهداف التكنولوجية ضمن الأهداف المحددة في استراتيجية المنظمة.

○ الأداء الإداري: يتعلق هذا الجانب بالخطط والسياسات والإجراءات التي تحددها المنظمة، ويتم تحقيق ذلك من خلال حسن اختيار أفضل البدائل التي تحقق أهداف المنظمة المخطط لها، ويمكن الاستعانة بالنماذج والأساليب العلمية لتطوير هذا الجانب بالإضافة إلى مراجعة الخطط الاستراتيجية للمنظمة لتحديد نقاط القوة والضعف.

3.2.2 مستويات الأداء:

توجد مجموعة من المستويات للأداء والذي يمكن لأي منظمة من خلاله معرفة مستوى أدائها، وتمثل هذه المستويات في:

1. الأداء الاستثنائي: يبين التفوق في الأداء المنظمة على المدى البعيد والعقود المربحة لها، وكذا الالتزام الواضح من قبل الأفراد، ووفرة السيولة، وازدهار الوضع المالي للمنظمة.
2. الأداء البارز يتم فيه الحصول على عدة عقود عمل كبيرة، وامتلاك إطارات ذات كفاءة، وامتلاك مركز ووضع مالي متميز.
3. الأداء الجيد جدا يبين مدى صلابة الأداء، واتضح الرؤية المستقبلية، إلى جانب التمتع بالوضع المالي الجيد.
4. الأداء الجيد يكون فيه تميز للأداء وفق المعدلات السائدة مع توازن نقاط القوة والضعف في المنتجات و / أو الخدمات وقاعدة العملاء، مع امتلاك وضع مالي مستقر.
5. الأداء المعتدل: يمثل صيرورة أداء دون المعدل، وتغلب نقاط الضعف على نقاط القوة في المنتجات و / أو الخدمات وقاعدة العملاء، مع صعوبة في الحصول على الأموال اللازمة للبقاء والنمو. (الجري، 2019)

4.2.2 محددات الأداء ومعوقاته:

• محددات الأداء: (Barbary, 2020)

الأداء هو الأثر الصافي لجهود الفرد التي تبدأ بالقدرات، وإدراك الدور والمهام، فهذا يعني أن الأداء هو نتاج للعلاقة المتداخلة بين كل من الجهد والقدرات، وإدراك الدور، والمهام المنوطة به فيشير الجهد إلى الطاقة الجسمية، والعقلية التي يبذلها الفرد لأداء مهمته وينتج هذا الجهد من حصول الفرد على حوافز تدفعه لذلك، أما القدرات فيقصد بها الصفات الشخصية للفرد والتي يستخدمها لأداء وظيفته، فيما يشير إدراك الدور أو المهمة إلى الاتجاه الذي يوجه الفرد جهوده في العمل من خلاله، ويتمثل ذلك في مجموعة الأنشطة والسلوكيات التي يقوم بها الفرد في أداء مهامه.

ولكي يحقق الفرد مستوى مرض من الأداء لابد من وجود تكامل وحد أدنى من الإتقان في كل مكون من مكونات الأداء، بمعنى أن الفرد إذا بذل جهودا فائقة، وكانت لديه قدرات لا بأس بها وكان مدركا لدوره فإن مستوى أدائه سيكون مقبولا، أما إذا كان يبذل جهودا كبيرة ويتمتع بقدرات متفوقة إلا أنه غير مدرك لدوره، أو أن لديه قدرات متفوقة والفهم اللازم للدور الذي يقوم به إلا أنه لا يبذل الجهود اللازمة.

في العمل فإن مستوى أدائه عادة ما يقيم كأداء منخفض أو غير مقبول، وفي بعض الأحيان قد يبذل العامل الجهد اللازم لذلك مع تمتعه بقدرات فائقة وفهما جيدا لمهمته إلا أنه يتصادم مع بعض العوامل الخارجية عن نطاق سيطرته يمكن لها أن تؤثر على مستوى أدائه. (الجرفي، 2019)

• معوقات الأداء

هناك بعض العوامل خارج نطاق سيطرة الفرد التي يمكن أن تؤثر على مستوى أدائه. وبالرغم من أن بعض هذه العوامل قد تؤخذ كأعذار، إلا أنها يجب أن تؤخذ في الاعتبار لأنها حقيقية وموجودة بالفعل، ومن أكثر عوائق الأداء شيوعا هي الإضاءة الحرارة، الضوضاء، التهوية، نمط الإشراف عدم الكفاية في تسهيلات العمل، والتركيبات والتجهيزات السياسات المحددة والتي تؤثر على الوظيفة، إلا أن هذه العوامل يطلق عليها العوامل الخارجية ليست وحدها المؤثرة على أداء العامل وإنتاجيته، ولكن يتفاعل معها العوامل

الداخلية والتي يمكن أن ترتبط بشخصية العامل ذكائه وقدراته الخاصة، سماته الشخصية وخبرته وتدريبه على ما يمارسه من عمل ظروف العمل الاجتماعية ويجب النظر إلى هذه العوامل البيئية على أنها مؤثرات على الجهد، القدرة والإتجاه فعلى سبيل المثال: أي عطل في أي آلة أو جهاز يمكن أن يؤثر بسهولة على الجهد الذي يبذله الفرد في العمل أيضا فإن السياسات غير الواضحة أو نمط الإشراف السيئ يمكن أن يسبب التوجيه الخاطئ للجهود، إضافة إلى أن النقص في التدريب يمكن أن يتسبب في إستغلال سيئ للقدرات الموجودة لدى الأفراد، لذا فإنه من أهم وأكبر مسؤوليات الإدارة الآتي: (غزال، 2022)

- توفير ظروف عمل مناسبة للعاملين.
- توفير بيئة تنظيمية مدعمة تقل فيها عوائق الأداء بما يمكن من تحقيق أداء جيد.
- عدم استخدام تقارير تقييم الاداء لنقد بعض العاملين بدفع العاملين الى اللجوء الى مواقف اندفاعية لإثبات أن الضعف في الاداء يرجع الى مدير المنظمة وانه ليس المسؤول عنها.
- عدم الحيز الشخصي لبعض ألف مرؤوسين دون البعض لأسباب غير مشروعة والتي ترتبط بالعمل.
- عدم استخدام أحد أنواع التقارير التقليدية والتي تكتفي بتقييم أحد الجوانب دون الأخرى.

5.2.2 أبعاد الأداء:

اختلف الباحثون والكتاب الإداريين على الأبعاد التي يركز عليها الاداء تبعا لتعريفهم، حيث يركز البعض على الجانب الاقتصادي في الأداء، بينما يعتمد البعض الآخر إلى الأخذ بالجانب التنظيمي والاجتماعي، وهذا من منطلق أن الأداء مفهوم شامل، وتتمثل هذه الأبعاد فيما يلي:

- أ. البعد التنظيمي للأداء: يقصد بالأداء التنظيمي الطرق والكيفيات التي تعتمد عليها المنظمة في المجال التنظيمي بغية تحقيق أهدافها، ومن ثم يكون لدى الإداريين في المنظمة معايير يتم على أساسها قياس فعالية الإجراءات التنظيمية المعتمدة وأثرها على الأداء، مع الإشارة إلى أن هذا القياس يتعلق مباشرة بالهيكل التنظيمية وليس بالنتائج المتوقعة ذات الطبيعة الاجتماعية الاقتصادية، وهذا يعني أنه بإمكان المنظمة أن تصل إلى مستوى فعالية آخر ناتج عن المعايير الاجتماعية والاقتصادية يختلف عن ذلك المتعلق بالفعالية التنظيمية.

ب. البعد الاجتماعي للأداء: يشير البعد الاجتماعي للأداء إلى مدى تحقيق الرضا عند أفراد المنظمة على اختلاف مستوياتهم، لأن مستوى رضا العاملين يعتبر مؤشراً على ولاء الأفراد لمؤسستهم، وتتجلى أهمية ودور هذا الجانب في كون أن الأداء الكلي للمنظمة قد يتأثر سلباً على المدى البعيد إذا اقتصرَت المنظمة على تحقيق الجانب الاقتصادي وأهملت الجانب الاجتماعي لمواردها البشرية، فكما هو معروف في أدبيات الإدارة أن جودة الإدارة في المنظمة ترتبط بمدى تلازم الفعالية الاقتصادية مع الفعالية الاجتماعية.

ونستنتج مما سبق أن هذه المعايير تلعب دوراً هاماً في تقوم الأداء، حيث تتيح للمنظمة إدراك الصعوبات التنظيمية في الوقت الملائم من خلال مظاهرها الأولى، قبل أن يتم إدراكها من خلال تأثيرها الاقتصادية، كما نعطي أهمية معتبرة للمناخ الاجتماعي السائد داخل المنظمة، أي لكل ما له صلة بطبيعة العلاقات الاجتماعية داخل المنظمة (صراعات، أزمات، ... الخ). (الجري، 2019)

6.2.2 العوامل المؤثرة في أداء المنظمة

إن تصنيف العوامل المؤثرة في أداء المنظمة يعد أمراً صعباً نظراً لتعددتها والترابط فيما بينها ودرجة تأثيرها في الأداء، فمن الباحثين من صنفها إلى مجموعة العوامل النفسية، والتكنولوجية، ومجموعة العوامل البشرية المتمثلة أساساً في المعرفة، التعليم، الخبرة التدريب المهارة القدرة الشخصية التكوين النفسي، ظروف العمل، حاجات ورغبات الأفراد، وهناك من صنف العوامل الأساسية المؤثرة في الأداء إلى التحفيز المهارات، مستوى العمل الممارسات.

وبما أن الأداء للعاملين يتأثر بكل مكونات ومحددات المنظمة، وكذلك يتأثر بالدوافع الفكرية والنفسية التي يمتلكها العاملين تجاه المنظمة، ويتأثر أيضاً بالوضع السياسي والاقتصادي والاجتماعي الذي تعيشه البيئة المحيطة، لذلك يصعب تحديد العوامل المؤثرة بالأداء الوظيفي تحديداً دقيقاً.

ويذكر البعض أنه يصعب تحديد العوامل المؤثرة كافة في فعالية الأداء للمنظمة لأنه مجال واسع ومتشعب الأبعاد، ولأن تلك العوامل متعددة يخضع بعضها لسيطرة الموظف بينما بعضها الآخر يخرج عن

سيطرتة، كما يعزى بعض الباحثين تلك الصعوبة الى القصور في فهم طبيعة التفاعل بين محددات الأداء، ويرجع بعض الباحثين صعوبة تحديد المؤثرات في فعالية الأداء للقيادة بصفة خاصة الى تداخل التفاعل بين شخصية القائد من ناحية، والأهداف والامكانيات المادية والبشرية ومدى قدرتها على تحقيق أهداف المنظمة واشباع حاجات العاملين والوفاء بمتطلبات المجتمع المحلي من ناحية رابعة، وعموماً يمكن تصنيف مختلف هذه العوامل الى نوعين:

1. عوامل خاضعة لتحكم المنظمة نسبياً: يكون هنا دور الإداريين هو زيادة تأثيراتها الايجابية والتقليل من تأثيراتها السلبية، ويمكن ذكر أهمها في التحفيز، والمهارات والتدريب والتكوين، وهي بمثابة عناصر رئيسية في تمكين العاملين وزيادة دافعيتهم وأدائهم.

ومن أبرز هذه العوامل أو المتغيرات التي تخضع لسيطرة المنظمة هي:

○ العوامل التقنية: وهي مختلف القوى والمتغيرات التي ترتبط بالجانب التقني في المنظمة، وتضم على الخصوص ما يلي:

- نوع التكنولوجيا سواء المستخدمة في الوظائف الفعلية أو المستخدمة في معالجة المعلومات.
- نسبة الاعتماد على الآلات بالمقارنة مع عدد العمال.
- تصميم المنظمة من حيث المخازن الورش والتجهيزات والآلات.
- نوعية المنتج، وشكله، ومدى مناسبة التغليف له.
- التوافق بين منتجات المنظمة ورغبات طالبيها.
- التناسب بين طاقتي التخزين والإنتاج في المنظمة.
- نوعية المواد المستخدمة في عملية الإنتاج ومستويات الأسعار.
- الموقع الجغرافي للمنظمة.

○ الهيكل التنظيمي: وهو الإطار الرسمي الذي يحدد درجة التخصص، وتقسيم العمل بين الوحدات والأفراد، وعدد المجموعات الوظيفية، وكذا عدد المستويات الإدارية، ولمن يتبع كل شخص ومن هم

الأشخاص الذين يتبعون له، وما هي سلطات ومسؤوليات كل منهم، وكيف يتم التنسيق بين وحداتها أو أقسامهما.

○ الموارد البشرية هي مختلف القوى والمتغيرات التي تؤثر على استخدام المورد البشري في المنظمة،

وتتضمن على وجه الخصوص:

- هيكل القوى العاملة.
- نظام الاختيار والتعيين.
- التدريب والتأهيل والتنمية.
- نظام الأجور والمكافآت.
- نظم تقييم الأداء.

2. العوامل غير الخاضعة لتحكم المنظمة: والمتعلقة عموماً بالمحيط الخارجي كالعوامل الاقتصادية

الاجتماعية، التكنولوجية وعوامل سياسية وقانونية بذلك يمكن القول أن الأداء هو دالة للعديد من

المتغيرات الكمية والنوعية، منها ما نستطيع التحكم فيه نسبياً، ومنها ما نجد صعوبة في ذلك، لهذا

تعددت الطرق والأدوات المستخدمة في تقييم الأداء وقياسه.

ومن بين العوامل التي تؤثر بشكل غير مباشر على المنظمة ما يلي:

○ العوامل السياسية: إن علاقة المنظمة بالمتغيرات السياسية تشمل جانب القرارات السياسية

كالحرب التأميمات الحظر على نشاط بعض المنظمات الانقلابات، كلها عوامل تؤثر على أداء

المنظمة.

○ العوامل الاقتصادية تشمل كل من معدلات الفائدة معدلات التضخم معدلات البطالة،

اتجاهات الأجور، توفر الطاقة وتكلفتها ... الخ.

○ العوامل الاجتماعية تتمثل في التركيبة السكانية التوزيع الجغرافي الأنماط الاستهلاكية، مستوى

التعليم ... الخ.

○ **العوامل التكنولوجية** وتشمل معدلات الإنفاق على البحوث والتطوير، تطور وسائل الاتصالات وأنظمة المعلومات والاختراعات الجديدة وغيرها من القوى التي تساهم في حل مشكلات العمل من خلال التقنيات الحديثة.

○ **العوامل البيئية والتشريعية** منها القوانين الخاصة بتنظيم علاقة المنظمة بالعاملين القوانين المرتبطة بالبيئة التي تعمل على حمايتها والمحافظة عليها من التلوث، القوانين الخاصة بالدفاع عن حقوق المستهلكين.

من أهم العوامل المؤثرة على الأداء، ما يلي:

1. غياب الأهداف المحددة: فالمنظمة التي لا تمتلك خطط تفصيلية لعملها وأهدافها، ومعدلات الإنتاج المطلوب أدائها، لن تستطيع قياس ما تحقق من إنجاز أو محاسبة موظفيها على مستوى أدائهم لعدم وجود معيار محدد مسبقاً لذلك، فلا تملك المنظمة معايير أو مؤشرات للإنتاج والأداء الجيد، فعندها يتساوى الموظف ذو الأداء الجيد مع الموظف ذو الأداء الضعيف.
2. عدم المشاركة في الإدارة: إن عدم مشاركة العاملين في المستويات الإدارية المختلفة في التخطيط وصنع القرارات يساهم في وجود فجوة بين القيادة الإدارية والموظفين في المستويات الدنيا، وبالتالي يؤدي إلى ضعف الشعور بالمسؤولية والعمل الجماعي لتحقيق أهداف المنظمة، وهذا يؤدي إلى تدني أو انخفاض مستوى الأداء لدى هؤلاء الموظفين لشعورهم بأنهم لم يشاركوا في وضع الأهداف المطلوب إنجازها أو في الحلول للمشاكل التي يواجهونها في الأداء، وقد يعتبرون أنفسهم مهمشين في المنظمة.
3. اختلاف مستويات الأداء: من العوامل المؤثرة على أداء الموظفين عدم نجاح الأساليب الإدارية التي تربط بين معدلات الأداء والمردود المادي والمعنوي الذي يحصلون عليه، فكلما ارتبط مستوى أداء الموظف بالترقيات والعلاوات والحوافز التي يحصل عليها كلما كانت عوامل التحفيز غير مؤثر بالعاملين، لهذا يجب اعداد نظاماً متميزاً لتقييم أداء الموظفين ليتم التمييز الفعلي بين الموظف المجتهد ذو الأداء العالي والموظف المجتهد ذو الأداء المتوسط والموظف الكسول والموظف غير المنتج.
4. مشكلات الرضى الوظيفي: فالرضا الوظيفي من العوامل الأساسية المؤثر على مستوى الأداء للموظفين، فعدم الرضى الوظيفي أو انخفاضه يؤدي إلى أداء ضعيف وإنتاجية أقل، والرضا الوظيفي

يتأثر بعدد كبير من العوامل التنظيمية والشخصية للموظف، مثل العوامل الاجتماعية كالسن والمؤهل التعليمي والجنس والعادات والتقاليد والعوامل التنظيمية كالمسؤوليات والوجبات ونظام الترقيات والحوافز في المنظمة.

5. التسبب الإداري: فالتسبب الإداري في المنظمة يعني ضياع ساعات العمل في أمور غير منتجة بل قد تكون مؤثرة بشكل سلبي على أداء الموظفين الآخرين، وقد ينشأ التسبب الإداري نتيجة لأسلوب القيادة أو الإشراف، أو للثقافة التنظيمية السائدة في المنظمة.

7.2.2 قياس وتحسين وتقييم الأداء

لقد بدأ الاهتمام بعملية قياس الأداء في الآونة الأخيرة تأخذ اهتماماً كبيراً نظراً لما يمثله ذلك من قدرة المنظمة على تقييم الممارسات الحالية ومدى ارتباطها بتحقيق الأهداف الموضوعية، وبعد قياس الأداء منهج استراتيجي أي يهدف إلى زيادة كفاءة أداء المنظمات من خلال تطوير أداء العاملين وفرق العمل وزيادة قدراتهم الإنتاجية. (غزال، 2022)

أولاً: قياس الأداء وأهميته:

منذ أكثر من قرن كتب اللورد كيفين قائلاً: عندما يكون بإمكانك قياس ما تحدث عنه وتعبّر عنه في صورة أرقام وأرقام، فإن ذلك يعني أنك تعرف شيئاً عنه، ولكنك عندما تعجز عن قياسه أو التعبير عنه في صورة عددية، يكون معنى ذلك أن معرفتك به ضئيلة أو غير مرضية، كما يضيف جينز "بأن ما يتم إخضاعه للقياس بالطريقة السليمة، يزداد احتمال أدائه بطريقة سليمة. إن قياس الأداء هو الوسيلة الصحيحة التي بواسطتها تحدد من خلال جميع العوامل المؤثرة في التقدم نحو الهدف بحيث يكون قياساً شاملاً لجميع أبعاد الأداء.

تعريف قياس الأداء:

يعرف قياس الأداء على أنه المراقبة المستمرة لإنجازات برامج المنظمة، وتسجيلها، وتوثيقها، ولا سيما مراقبة وتسجيل جوانب سير التقدم نحو تحقيق غايات موضوعية مسبقاً.

ويعد قياس الأداء منهج استراتيجي أي يهدف إلى زيادة كفاءة أداء المنظمات من خلال تطوير أداء العاملين وخلق العمل وزيادة قدراتهم الإنتاجية، وعادة ما تكون الجهة التي تقوم بإجراء عملية قياس الأداء هي الإدارة المسؤولة عن مفردات عناصر برامج المنظمة. (غزال، 2022)

أهمية قياس الأداء:

من أهمية قياس الأداء في أنه يوفر معلومات عن الكيفية التي تؤدي بها الأعمال وهل هي جيدة أم لا، إلى جانب توفيره معلومات تفيد في تحديد مسؤولية أداء تلك الأعمال، وإجراءات المحاسبة والمساءلة عن الأخطاء، كما يوفر كذلك معلومات تمكن من تطوير أداء الأفراد لأعمالهم ولسلوكلهم.

وتتمثل أهداف فوائد قياس الأداء الآتي:

1. تؤدي عملية قياس الأداء إلى تحقيق فوائد كثيرة للمنظمة، حيث أنها توفر مدخلا واضحا للتركيز على الخطة الإستراتيجية للبرامج، فضلا عن غاياته ومستوى أدائه.
2. يوفر قياس الأداء آلية معينة لرفع التقارير حول أداء برنامج العمل إلى الإدارة العليا
3. يركز قياس الأداء على الاهتمام بما يجب إنجازه، ويحفز المنظمات على توفير الوقت والموارد والطاقة اللازمة لتحقيق الأهداف.
4. كما يؤدي قياس الأداء إلى تحسين إدارة المنتجات والخدمات وعملية إيصالها إلى العملاء.
5. ويساعد قياس الأداء أيضا على تبرير تنفيذ البرامج وتكاليفها.
6. كما أنه يشجع على التوجه بشكل بناء نحو حل المشاكل.
7. العمل على رفع الروح المعنوية للعاملين.
8. وسيلة لتطوير الاداء الذاتي.
9. الكشف عن الاحتياجات التدريبية.

تحسين الأداء:

ان عملية تحسين الأداء من الوظائف الأساسية والاستراتيجية في المنظمة، وتهدف المنظمة من خلالها إلى أداء مواردها البشرية ومن ثم أدائها العام، وهي في الواقع تشكل نظام يتم عبر خطوات مترابطة، ونظرا لأهمية هذا النظام وتأثيره على عدد من الأطراف الفاعلة في المنظمة يتوجب على المنظمة بصفة عامة وإدارة الموارد البشرية بشكل خاص القيام بمراقبة الأداء والبحث عن سبل تحسينه ، والتأكد من قيامه بالأهداف المرجوة منه على أكمل وجه، وهذا من خلال التأكد من توفره على الشروط الواجبة في أنظمة التقييم والتحسين السليمة والفعالة. (غزال، 2022)

مفهوم تحسين الأداء:

إن تحسين الأداء هو استخدام جميع الموارد المتاحة لتحسين المخرجات وإنتاجية العمليات، وتحقيق التكامل بين التكنولوجيا الصحيحة التي توظف رأس المال بالطريقة المثلى، ومن المبادئ الأساسية لتحسين الأداء:

1. الوعي بتحقيق احتياجات وتوقعات الزبون (داخلي خارجي)
2. إزالة الحواجز والعوائق وتشجيع مشاركة جميع العاملين
3. التركيز على النظم والعمليات.
4. القياس المستمر ومتابعة الأداء.

الفصل الثالث: منهجية الدراسة وإجراءاتها

تمهيد:

هدف البحث الحالي إلى دراسة أثر المخاطر الإلكترونية بأبعادها المختلفة على تحقيق أداء شركات في شركات التقنية بمدينة الرياض ويتناول هذا الفصل وصف لإجراءات البحث الميدانية التي قام بها الباحث لتحقيق أهداف البحث، وتتضمن تحديد المنهج المتبع في البحث، ومجتمع البحث، وعينة البحث، وأداة البحث والتحقق من صدقها وثباتها، والمعالجة الإحصائية المستخدمة في تحليل النتائج.

1.3 منهج الدراسة:

اعتمدت هذه الدراسة على المنهج الوصفي التحليلي، والذي يُعد من أكثر المناهج البحثية ملاءمة لدراسة العلاقة بين المتغيرات وتفسير تأثيرها. يهدف هذا المنهج إلى وصف الظاهرة المدروسة وتحليلها من خلال جمع البيانات من عينة الدراسة، ثم استخدام الأساليب الإحصائية لاختبار الفرضيات واستنتاج العلاقة بين المخاطر الإلكترونية و أداء شركات في شركات التقنية بمدينة الرياض ..

2.3 مجتمع البحث وعينته:

يتكوّن مجتمع الدراسة من العاملين في شركات التقنية بمدينة الرياض، باعتبارها من أكثر القطاعات عرضة للمخاطر الإلكترونية نظراً لاعتمادها الكبير على البنية التحتية الرقمية والأنظمة التقنية المتقدمة. ويشمل هذا المجتمع الموظفين في الإدارات المختلفة كالإدارة العامة، التقنية، الهندسية، والدعم الفني، ممن لديهم إلمام مباشر بتأثير التهديدات السيبرانية على الأداء المؤسسي، وقد تم اختيار هذا المجتمع لكونه يمثل بيئة خصبة لفحص العلاقة بين المخاطر الإلكترونية وأداء الشركات، خاصة في ظل التوسع الرقمي الكبير الذي تشهده المملكة.

ونظرًا لصعوبة حصر مجتمع الدراسة المتمثل في جميع العاملين في شركات التقنية بمدينة الرياض، وبسبب اتساع حجم المجتمع وتوزعه على عدد كبير من الشركات والمؤسسات، تم اعتماد العينة العشوائية البسيطة كإحدى أكثر أدوات المعاينة ملائمة وحيادية لجمع البيانات من الأفراد بطريقة تضمن تكافؤ الفرص في تمثيل المجتمع الأصلي، وقام الباحث بتوزيع عدد 370 استبانة إلكترونيًا وورقيًا على أفراد العينة المستهدفة، ممن يعملون في قطاعات إدارية وتقنية مختلفة داخل شركات التقنية، وتم استرجاع عدد 318 استبانة صالحة للتحليل الإحصائي، بنسبة استرداد بلغت تقريبًا 85.9%، وهو معدل مرتفع يعكس جدية المشاركين وجودة أدوات جمع البيانات.

3.3 أداة الدراسة:

بعد أن تم الاطلاع على الدراسات السابقة المتعلقة بموضوع البحث والاستعانة بالإطار النظري للبحث، قام الباحث ببناء وتطوير الاستبيان كأداة لجمع بيانات الدراسة؛ لمناسبتها لتحقيق أهداف الدراسة، والإجابة عن تساؤلاتها

4.3 بناء أداة الدراسة:

تعتمد هذه الدراسة على الاستبيان كأداة رئيسية لجمع البيانات، حيث تم تصميمه بدقة لقياس أثر المخاطر الإلكترونية بأبعادها المختلفة على تحقيق أداء شركات في شركات التقنية بمدينة الرياض. وقد تم تطوير الاستبيان استنادًا إلى الدراسات السابقة والمفاهيم النظرية ذات الصلة، مع مراعاة تحقيق الصدق والثبات لضمان دقة النتائج، حيث تكونت أداة الدراسة من جزأين رئيسيين، على النحو التالي:

❖ القسم الأول: المعلومات الديموغرافية

❖ القسم الثاني: المخاطر الإلكترونية

• يقيس هذا القسم جودة المخاطر الإلكترونية، ويتضمن 3 أبعاد رئيسية، وهي: (مخاطر أمن

المعلومات - مخاطر الاحتيال - مخاطر عدم رضا العملاء)

❖ القسم الثالث: أداء شركات

مقياس ليكرت الخماسي:

كانت الإجابة عن فقرات الاستبيان في ضوء مقياس خماسي على النحو التالي:

جدول رقم (1) مفتاح التصحيح

الإجابة	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
الدرجة	5	4	3	2	1

5.3 صدق أداة الدِّراسة:

إن صدق الأداة يعني التأكُّد من أنها سوف تقيس ما أعدت لقياسه، كما يُقصد بالصدق "شمول الأداة لكل العناصر التي يجب أن تدخل في التحليل من ناحية، ووضوح فقراتها ومفرداتها، وقد قام الباحث بالتأكُّد من صدق أداة الدِّراسة من خلال القيام بما يلي:

الصدق الظاهري للأداة (التحكيبي):

بعد الانتهاء من بناء أداة الدِّراسة، تمَّ عرضها على عدد من أعضاء هيئة التدريس المتخصِّصين؛ وذلك للاسترشاد بأرائهم، وقد طُلب من المحكِّمين إبداء الرأي حول مدى وضوح العبارات، ومدى ملاءمتها لما وُضعت لأجله، ومدى مناسبة العبارات للمحور الذي تنتمي إليه، مع وضع التعديلات والاقتراحات التي يمكن من خلالها تطوير الاستبانة.

صدق الاتساق الداخلي:

بعد التأكُّد من الصدق الظاهري لأداة الدِّراسة قام الباحث بالتأكُّد من صدق الاتساق الداخلي وتم حساب الصدق الداخلي لفقرات الاداة، حيث تم حساب معامل الارتباط بين إجابات العينة على كل

فقرة والدرجة الكلية للمحور الذي تنتمي اليه، وذلك باستخدام برنامج (SPSS)، حيث جاءت النتائج على النحو التالي:

➤ المحور الأول: المخاطر الإلكترونية

جدول (2) معاملات الارتباط لمحور المخاطر الإلكترونية :

مخاطر أمن المعلومات	مخاطر الاحتيال	مخاطر عدم رضا العملاء
مخاطر أمن المعلومات	0.785	0.748
مخاطر الاحتيال	1.000	0.819
مخاطر عدم رضا العملاء	0.819	1.000

يوضح الجدول أن هناك علاقة ارتباط إيجابية قوية بين مخاطر الاحتيال ومخاطر عدم رضا العملاء (0.819)، مما يشير إلى أن تحسين الجدولة الزمنية يساهم في ضبط التكاليف بشكل فعال. كذلك، توجد علاقة ارتباط إيجابية عالية بين مخاطر أمن المعلومات ومخاطر الاحتيال (0.785)، مما يعكس تأثير تحديد النطاق الدقيق على تحسين جدولة المشروع. بينما العلاقة بين مخاطر أمن المعلومات ومخاطر عدم رضا العملاء (0.748) تظهر ارتباطاً جيداً، مما يعني أن وضوح النطاق يساعد في تحسين إدارة التكاليف. من ناحية أخرى، يوجد ارتباط ضعيف سلبي بين إدارة الجودة ومخاطر عدم رضا العملاء (-0.288)، مما قد يشير إلى تحديات في تحقيق الجودة دون زيادة في التكاليف. كما أن العلاقة بين إدارة الجودة ومخاطر أمن المعلومات (-0.196) ضعيفة وسلبية، مما قد يعني أن التركيز على الجودة قد يؤدي أحياناً إلى تعديلات في نطاق المشروع. وأخيراً، العلاقة بين إدارة الجودة ومخاطر الاحتيال (0.250) ضعيفة ولكنها إيجابية، مما يشير إلى أن تحسين الجدولة قد يعزز جودة التنفيذ.

6.3 ثبات أداة الدراسة:

لقياس ثبات أداة الدراسة، تم استخدام معامل ألفا كرونباخ (Cronbach's Alpha) لقياس مدى اتساق الفقرات في الاستبيان ودرجة موثوقية الأداة البحثية. ويعتبر معامل الثبات مرتفعاً إذا كان

أكبر من 0.70، مما يدل على أن الأداة البحثية موثوقة ويمكن الاعتماد عليها في قياس المتغيرات المختلفة للدراسة.

جدول (3) معاملات ألفا كرونباخ لمحاور الدراسة

المحور	عدد الفقرات	معامل ألفا كرونباخ	درجة الثبات
المخاطر الإلكترونية	25	0.89	مرتفع جداً
أداء شركات	10	0.87	مرتفع
الأداة ككل	35	0.91	مرتفع جداً

تشير النتائج إلى أن جميع قيم معامل ألفا كرونباخ أعلى من 0.80، مما يدل على أن أداة الدراسة تتمتع بدرجة عالية من الثبات والاتساق الداخلي، وبالتالي يمكن الوثوق في نتائج التحليل الإحصائي والاستنتاجات التي سيتم التوصل إليها.

7.3 أساليب تحليل البيانات:

تم الاعتماد على مجموعة من الأساليب الإحصائية لتحليل بيانات الدراسة، وذلك باستخدام برنامج SPSS لضمان دقة النتائج وتحقيق أهداف البحث. وقد شملت أساليب التحليل ما يلي::

- التكرارات والنسب المئوية (Percentage & Frequencies): للتعرف على الخصائص الشخصية لأفراد عينة الدراسة.
- المتوسط الحسابي (Mean): لمعرفة مدى ارتفاع أو انخفاض إجابات أفراد عينة الدراسة عن المحاور الرئيسية (متوسط متوسطات العبارات).
- الانحراف المعياري (Standard Deviation): للتعرف على مدى انحراف إجابات أفراد عينة الدراسة لكل عبارة من عبارات متغيرات الدراسة، ولكل محور من المحاور الرئيسية عن متوسطها الحسابي، وقد استخدمت الدراسة هذا الأسلوب نظراً لأن الانحراف المعياري يوضح التشتت في

إجابات أفراد عينة الدراسة لكل عبارة من عبارات متغيرات الدراسة، إلى جانب المحاور الرئيسة،

فكلما اقتربت قيمته من الصفر تركزت الاجابات وانخفض تشتتها بين المقياس.

■ معامل ارتباط بيرسون (Pearson): لقياس الاتساق الداخلي بين عبارات الأداة (الاستبانة) وكل

محور تنتهي إليه.

■ معامل الثبات ألفا كرونباخ (cronbach's Alpha- α): لحساب معامل ثبات أداة الدراسة

■ اختبار تحليل الانحدار (Regression Test) للتحقق من فروض الدراسة

الفصل الرابع: نتائج الدِّراسة وتفسيرها

المقدمة

يتناول هذا الفصل عرضًا للنتائج التي توصّلت إليها الدِّراسة الحاليّة، وذلك من خلال عرض استجابات أفراد عينة الدِّراسة لعبارات الأداة، ومعالجتها إحصائيًّا، وصولًا إلى النتائج وتحليلها وتفسيرها، في ضوء الأطر النظريّة، والدِّراسات السابقة المتعلقة بموضوع الدراسة، ويقوم الباحث بمناقشة النتائج التي توصّلت إليها الدِّراسة وتفسيرها، من خلال الإجابة عن أسئلتها والتحقق من فروضها

1.4 خصائص عينة الدِّراسة:

تم حساب التكرارات والنسب المئوية لأفراد عينة البحث وفقاً للمتغيرات:

جدول (4): توزيع أفراد عينة الدراسة حسب الخصائص الديموغرافية (حجم العينة = 318)

الفئة	التكرار	النسبة المئوية (%)
النوع		
ذكر	176	55.48
أنثى	142	44.52
العمر		
أقل من 30 سنة	77	24.19
30-40 سنة	118	37.10
41-50 سنة	87	27.42
أكثر من 50 سنة	36	11.29
المستوى التعليمي		

15.48	49	ثانوي فأقل
48.39	154	بكالوريوس
24.19	77	ماجستير
11.94	38	دكتوراه
عدد سنوات الخبرة		
20.97	67	أقل من 5 سنوات
33.87	108	5-10 سنوات
27.42	87	11-15 سنة
17.74	56	أكثر من 15 سنة
الوظيفة		
29.03	92	إداري
25.81	82	مهندس
24.19	77	تقني
20.97	67	أخرى

يُظهر الجدول توزيع أفراد عينة الدراسة وفقاً للخصائص الديموغرافية بعد تعديل حجم العينة إلى 318 شخصاً. يعكس هذا التوزيع توازناً نسبياً بين الذكور والإناث، حيث يشكل الذكور 55.48% من العينة والإناث 44.52%. هذا يشير إلى تنوع عادل في الجنس بين أفراد العينة.

بالنسبة للفئة العمرية، تهيمن الفئة العمرية من 30 إلى 40 سنة على العينة بنسبة 37.10%، تليها فئة 41-50 سنة بنسبة 27.42%. أما الفئات الأصغر (أقل من 30 سنة) والأكبر (أكثر من 50 سنة) فتشكلان نسباً أقل، مما يعكس تنوعاً في الخبرات العمرية لأفراد العينة.

فيما يتعلق بالمستوى التعليمي، تمثل فئة الحاصلين على درجة البكالوريوس أكبر شريحة من العينة بنسبة 48.39%، تليها فئة الحاصلين على شهادة الماجستير بنسبة 24.19%. أما الحاصلون على

شهادة الدكتوراه فيشكلون نسبة أقل (11.94%)، مما يشير إلى تمركز عينة الدراسة بشكل أكبر في فئة الحاصلين على درجات علمية متوسطة.

أما بالنسبة لعدد سنوات الخبرة، تمثل فئة الذين لديهم خبرة من 5 إلى 10 سنوات أكبر شريحة من العينة بنسبة 33.87%، تليها فئة الذين لديهم خبرة من 11 إلى 15 سنة بنسبة 27.42%. فئات الخبرة الأقل من 5 سنوات والأكثر من 15 سنة تشكلان نسباً أقل، مما يشير إلى أن العينة تضم بشكل رئيسي أفراداً ذوي خبرة متوسطة.

بالنسبة للوظيفة، تُعد الفئة الإدارية أكبر الفئات بنسبة 29.03%، تليها الفئة الهندسية بنسبة 25.81%. الفئة التقنية تمثل 24.19%، بينما تمثل الفئة الأخرى 20.97%. هذه النسب توضح تنوعاً في الخلفيات الوظيفية للعينة، مما يعزز من تنوع البيانات المستخلصة.

2.4 دراسة محاور الاستبيان:

■ المحور الأول المخاطر الإلكترونية

لدراسة محور المخاطر الإلكترونية : تمّ حساب المتوسطات الحسابية والانحرافات المعيارية لأبعاد المحور الأول كما يلي

البعد الأول مخاطر أمن المعلومات

جدول (5) المتوسطات الحسابية والانحرافات المعيارية والترتيب لعبارات بعد مخاطر أمن المعلومات

رقم الفقرة	الفقرة	المتوسط الحسابي	الانحراف المعياري	الرتبة	درجة الموافقة
	تحيي المعلومات من الوصول غير المصرح به، مما يضمن سرية	4.50	0.70	1	موافق بشدة

				البيانات ويحافظ على خصوصية الأفراد والمؤسسات.	
موافق بشدة	2	0.75	4.42	يستخدم تقنيات تشفير فعالة لضمان حماية البيانات الحساسة، مما يمنع تسريب المعلومات أثناء انتقالها عبر الشبكات.	2
موافق بشدة	3	0.80	4.35	يطبق أنظمة أمنية لحماية الشبكات من الهجمات الخارجية، مما يساهم في تقليل خطر الاختراقات والتهديدات المتزايدة.	3
موافق	4	0.85	4.30	يحدث الأنظمة الأمنية بشكل دوري لمواكبة التهديدات الحديثة، الأمر الذي يعزز القدرة على التصدي للمخاطر الإلكترونية المستجدة.	4
موافق	5	0.90	4.25	يوفر برامج تدريبية للموظفين بشأن مخاطر أمن المعلومات، مما يعزز وعيهم ويؤهلهم للتعامل مع التهديدات الإلكترونية بفعالية.	5
موافق بشدة		0.78	4.36	المتوسط العام	

يوضح الجدول أن متوسطات الحسابية لفقرات "مخاطر أمن المعلومات" تتراوح بين 4.25 و 4.50، مما يعكس درجة عالية من الموافقة من المشاركين على هذه الإجراءات الأمنية. جميع الفقرات حصلت على متوسطات تتجاوز 4.0، مما يشير إلى أن الأفراد في العينة يميلون بشدة إلى تأييد هذه التدابير كجزء أساسي من استراتيجيات الحماية الأمنية في مؤسساتهم. كما أن الانحرافات المعيارية تراوحت بين 0.70 و 0.90، مما

يدل على أن هناك تباينًا بسيطًا في آراء المشاركين، حيث تتجمع أغلب الآراء حول هذه الممارسات الأمنية ولا توجد تباينات كبيرة في مدى توافق الأفراد مع أهمية هذه التدابير.

وتظهر الفقرة الأولى، التي تتعلق بحماية المعلومات من الوصول غير المصرح به، حصلت على أعلى تقييم (4.50) مع انحراف معياري منخفض (0.70)، مما يشير إلى أن أغلب المشاركين يتفقون بقوة مع هذه الممارسة الأمنية ويعتقدون بأنها من الأولويات الكبرى في حماية البيانات، وحصلت الفقرة الخامسة، المتعلقة بتوفير برامج تدريبية للموظفين بشأن مخاطر أمن المعلومات، على أقل تقييم (4.25) مع انحراف معياري أعلى (0.90)، مما قد يشير إلى وجود تباين أكبر في آراء المشاركين حول مدى كفاية برامج التدريب ومدى تأثيرها في رفع الوعي الأمني داخل المؤسسات..

البعد الثاني مخاطر الاحتيال

جدول (6) المتوسطات الحسابية والانحرافات المعيارية والترتيب لعبارات بعد مخاطر الاحتيال

رقم الفقرة	الفقرة	المتوسط الحسابي	الانحراف المعياري	الرتبة	درجة الموافقة
6	تحديد الأساليب الاحتيالية الحديثة التي قد تهدد النظام المالي	4.15	0.88	2	موافق
7	تعزيز السياسات والإجراءات لمكافحة محاولات الاحتيال المالي	4.25	0.80	1	موافق بشدة
8	مراقبة الأنشطة المشبوهة داخل الأنظمة المالية لرصد الاحتيال	4.10	0.92	3	موافق

9	تطبيق أنظمة متقدمة للكشف عن الأنشطة الاحتيالية في البيانات المالية	4.05	0.95	4	موافق
10	توفير برامج تدريبية مستمرة للموظفين حول أساليب الاحتيال وطرق مكافحتها	4.00	1.00	5	موافق
المتوسط العام		4.11	0.91	موافق	

يوضح الجدول أن المشاركين في الدراسة أبدوا موافقة قوية على أهمية الإجراءات التي تهدف إلى مكافحة الاحتيال المالي، حيث تراوحت المتوسطات الحسابية بين 4.00 و 4.25. حصلت الفقرة السابعة، التي تتعلق بتعزيز السياسات والإجراءات لمكافحة محاولات الاحتيال المالي، على أعلى تقييم بمتوسط 4.25، مما يعكس توافقاً قوياً مع ضرورة تحسين السياسات والإجراءات الوقائية ضد الاحتيال المالي. كما أن الفقرة السادسة، التي تتعلق بتحديد الأساليب الاحتيالية الحديثة، حصلت على تقييم 4.15، ما يشير إلى أهمية مواكبة الأساليب الاحتيالية الحديثة والتكيف معها.

من ناحية أخرى، حصلت الفقرة العاشرة المتعلقة بتوفير برامج تدريبية مستمرة للموظفين على أدنى تقييم (4.00)، مع انحراف معياري مرتفع (1.00)، مما يدل على وجود تباين أكبر في آراء المشاركين حول فعالية برامج التدريب المتاحة. يشير هذا إلى أن المشاركين قد يختلفون في تقدير كفاءة هذه البرامج في تحضير الموظفين لمواجهة أساليب الاحتيال. بشكل عام، يمكن القول إن المشاركين يوافقون على الإجراءات الوقائية ضد الاحتيال، مع التركيز على أهمية تعزيز السياسات والتدريب المستمر لمكافحة الاحتيال المالي.

البعد الثالث مخاطر عدم رضا العملاء

جدول (7) المتوسطات الحسابية والانحرافات المعيارية والترتيب لعبارات بعدد مخاطر عدم رضا

العملاء

رقم الفقرة	الفقرة	المتوسط الحسابي	الانحراف المعياري	الرتبة	درجة الموافقة
11	تحديد العوامل التي تؤدي إلى عدم رضا العملاء وتحليل تأثيرها على السمعة المؤسسية	4.32	0.72	2	موافق بشدة
12	تحسين جودة الخدمة المقدمة للعملاء لتقليل احتمالات عدم رضاهم	4.38	0.70	1	موافق بشدة
13	مراقبة شكاوى العملاء بشكل دوري وتقديم حلول سريعة وفعالة	4.10	0.90	4	موافق
14	تعزيز قنوات التواصل مع العملاء لضمان فهم احتياجاتهم ومتطلباتهم	4.25	0.85	3	موافق بشدة
15	توفير استراتيجيات للتعامل مع الشكاوى والعمل على تحسين الخدمة بناءً عليها	4.05	0.95	5	موافق
	المتوسط العام	4.22	0.80		موافق بشدة

تُظهر النتائج أن المشاركين أبدوا موافقة قوية على معظم الإجراءات المرتبطة بمخاطر عدم رضا العملاء، حيث تراوحت المتوسطات الحسابية بين 4.05 و 4.38. حصلت الفقرة الثانية عشرة، التي تناولت "تحسين جودة الخدمة المقدمة للعملاء"، على أعلى تقييم (4.38) مع انحراف معياري منخفض (0.70).

مما يدل على توافق واسع بين المشاركين في أهمية تحسين جودة الخدمة كإجراء رئيسي للحد من عدم رضا العملاء.

أما الفقرة الحادية عشرة التي تتعلق بـ "تحديد العوامل التي تؤدي إلى عدم رضا العملاء"، فقد حصلت على تقييم 4.32، مما يعكس أيضًا أهمية كبيرة لتحديد ومعالجة الأسباب الرئيسية لعدم رضا العملاء بشكل دقيق. من ناحية أخرى، سجلت الفقرة الخامسة، التي تناولت "توفير استراتيجيات للتعامل مع الشكاوى وتحسين الخدمة بناءً عليها"، أدنى تقييم (4.05)، مما يشير إلى أن بعض المشاركين قد يرون أن هذه الاستراتيجيات قد تحتاج إلى مزيد من التطوير لضمان فعالية التعامل مع شكاوى العملاء.

ومما سبق يتبين أن المخاطر الإلكترونية جاءت كما يلي

الرقم	البعد	المتوسط الحسابي	الانحراف المعياري	الرتبة	درجة الموافقة
	مخاطر أمن المعلومات	4.10	0.91	4	موافق
2	مخاطر الاحتيال	4.11	0.91	3	موافق بشدة
3	مخاطر عدم رضا العملاء	4.22	0.80	2	موافق بشدة
	المتوسط العام	4.14	0.85		موافق

يوضح الجدول ترتيب أبعاد المخاطر الإلكترونية بناءً على المتوسط الحسابي للموافقة على كل بعد. جاءت "مخاطر أمن المعلومات" في المرتبة الرابعة بمتوسط حسابي قدره 4.10 وانحراف معياري 0.91، مما يشير إلى أن المشاركين يعترفون بأهمية المخاطر المرتبطة بأمن المعلومات، ولكن بموافقة أقل مقارنة بالأبعاد الأخرى. يشير هذا إلى أن هناك حاجة ملحة لمزيد من التحسينات في تدابير حماية المعلومات وأمن الشبكات.

في المرتبة الثالثة، جاءت "مخاطر الاحتيال" بمتوسط حسابي قدره 4.11، مما يعكس موافقة قوية على ضرورة مواجهة هذه المخاطر. وبالنسبة لهذه المخاطر، يعتبر المشاركون أن تطبيق الأنظمة الوقائية والرقابية لمكافحة الاحتيال المالي يعد خطوة أساسية لحماية المؤسسات.

أما "مخاطر عدم رضا العملاء"، فقد حصلت على أعلى تقييم بين الأبعاد الثلاثة بمتوسط حسابي قدره 4.22 وانحراف معياري منخفض قدره 0.80، مما يعكس توافقاً قوياً بين المشاركين على أن عدم رضا العملاء يشكل تهديداً رئيسياً ويجب اتخاذ الإجراءات الفعالة للحد منه. يشير هذا إلى أن المشاركين يضعون أهمية كبيرة على تحسين تجربة العملاء وضمان رضاهم في مواجهة المخاطر الإلكترونية..

■ المحور الثاني أداء شركات

جدول (8) المتوسطات الحسابية والانحرافات المعيارية والترتيب لعبارات المحور الثاني

رقم الفقرة	الفقرة	المتوسط الحسابي	الانحراف المعياري	الرتبة	درجة الموافقة
1	تؤثر المخاطر الإلكترونية على قدرة المنظمة على تحقيق أهدافها الاستراتيجية بشكل سلبي.	3.84	0.967	8	موافق
2	تعرض الشركة للمخاطر الإلكترونية يعيق بشكل ملحوظ تحسين كفاءة العمليات الداخلية.	3.83	0.966	9	موافق
3	تؤدي المخاطر الإلكترونية إلى زيادة التكاليف التشغيلية بسبب استجابة المنظمة للحوادث الأمنية.	4.33	0.636	3	موافق بشدة

4	تؤثر المخاطر الإلكترونية بشكل مباشر على الابتكار في منتجات أو خدمات الشركة.	4.19	0.751	4	موافق
5	تؤدي المخاطر الإلكترونية إلى تباطؤ في اتخاذ القرارات الاستراتيجية داخل المنظمة.	4.41	0.636	1	موافق بشدة
6	تؤثر المخاطر الإلكترونية بشكل سلبي على رضا العملاء والعلاقات مع الموردين.	4.07	0.959	6	موافق
7	تؤدي المخاطر الإلكترونية إلى تأخير أو توقف في تحقيق الأهداف المالية المحددة.	4.05	0.846	7	موافق
8	يؤدي التعامل غير الفعال مع المخاطر الإلكترونية إلى انخفاض في إنتاجية الموظفين.	4.25	0.710	5	موافق بشدة
9	المخاطر الإلكترونية تؤثر على سمعة الشركة في السوق وبالتالي تقلل من قدرتها على جذب العملاء الجدد.	3.95	0.890	10	موافق
10	تؤدي المخاطر الإلكترونية إلى تأثير سلبي على ثقافة العمل داخل المنظمة.	4.30	0.650	2	موافق بش

المتوسط العام	—	4.10	0.82	—	موافق
---------------	---	------	------	---	-------

يظهر أن هناك توافقاً قوياً بين المشاركين حول تأثير المخاطر الإلكترونية على أداء الشركات، حيث تراوحت المتوسطات الحسابية بين 3.83 و 4.41. الفقرة التي تتعلق بتباطؤ اتخاذ القرارات الاستراتيجية نتيجة للمخاطر الإلكترونية (الفقرة 5) حصلت على أعلى متوسط حسابي (4.41) مع انحراف معياري منخفض قدره 0.636، مما يشير إلى اتفاق قوي بين المشاركين على أن المخاطر الإلكترونية تشكل عائقاً كبيراً أمام اتخاذ القرارات الاستراتيجية.

أما الفقرة المتعلقة بزيادة التكاليف التشغيلية بسبب استجابة المنظمة للحوادث الأمنية (الفقرة 3) فقد سجلت أيضاً متوسطاً مرتفعاً (4.33)، مما يدل على أن المشاركين يعتبرون هذه التأثيرات من المخاطر الإلكترونية مهمة على مستوى التكاليف. في المقابل، حصلت الفقرة التي تتعلق بتأثير المخاطر الإلكترونية على سمعة الشركة في السوق (الفقرة 9) على أقل تقييم (3.95) مع انحراف معياري (0.890)، مما يشير إلى أن التأثير على السمعة وجذب العملاء الجدد يُعتبر أقل أهمية نسبياً مقارنة ببقية التأثيرات.

3.4 فرضيات الدراسة

الفرضية الرئيسة: لا يوجد أثر دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) للمخاطر الإلكترونية (مخاطر أمن المعلومات، مخاطر الاحتيال، مخاطر عدم رضا العملاء) على أداء شركات في شركات التقنية بمدينة الرياض

للتحقق من صحة هذا الفرض تم استخدام تحليل الانحدار المتعدد (Regression test)، وجاءت

النتائج كما بالجدول التالي:

جدول (9) أثر المخاطر الإلكترونية على أداء شركات في شركات التقنية بمدينة الرياض

المتغيرات المستقلة	معاملات الانحدار	قيمة اختبار T	مستوى الدلالة
المقدار الثابت	0.482	3.142	0.002
مخاطر أمن المعلومات	-0.162	-2.874	0.005
مخاطر الاحتيال	0.627	2.920	0.002
مخاطر عدم رضا العملاء	0.535	8.512	0.000
معامل الارتباط = 0.897		معامل التحديد = 0.800	
قيمة الاختبار F = 160.304		القيمة الاحتمالية = 0.00	

يظهر من الجدول أن المشاركين يوافقون بشكل عام على أن المخاطر الإلكترونية تؤثر بشكل كبير على أداء الشركات، حيث تتراوح المتوسطات الحسابية بين 3.83 و 4.41. الفقرة المتعلقة بتأثير المخاطر الإلكترونية على تباطؤ اتخاذ القرارات الاستراتيجية داخل الشركة حصلت على أعلى تقييم (4.41) مع انحراف معياري منخفض (0.636)، مما يدل على توافق قوي من المشاركين حول تأثير المخاطر الإلكترونية على قدرة الشركات في اتخاذ قرارات استراتيجية فعالة. كما حصلت الفقرة المتعلقة بزيادة التكاليف التشغيلية نتيجة استجابة المنظمة للحوادث الأمنية على تقييم مرتفع (4.33) مما يعكس إدراكاً واضحاً للمشاركين بأن المخاطر الإلكترونية ترفع التكاليف بشكل ملحوظ.

من ناحية أخرى، سجلت الفقرة المتعلقة بتأثير المخاطر الإلكترونية على سمعة الشركة في السوق (3.95) أدنى تقييم، مع انحراف معياري (0.890)، مما يشير إلى تباين في الآراء حول تأثير هذه المخاطر على سمعة الشركة وجذب العملاء الجدد. على الرغم من أن المخاطر الإلكترونية تؤثر بشكل ملحوظ على جوانب أخرى مثل القرارات الاستراتيجية والتكاليف التشغيلية، إلا أن المشاركين يرون أن تأثيرها على السمعة ليس بنفس القوة، وهو ما يعكس الحاجة إلى مزيد من الفهم حول العلاقة بين المخاطر الإلكترونية وسمعة الشركة في السوق.

ويتفرع منه الفروض التالية

- الفرض الفرعي الأول لا يوجد أثر ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) لبعدهم مخاطر أمن المعلومات على أداء شركات في شركات التقنية بمدينة الرياض .

للتحقق من صحة هذا الفرض تم استخدام تحليل الانحدار الخطي البسيط (Linear Regression test)، وجاءت النتائج كما بالجدول التالي:

جدول (10) أثر لبعدهم مخاطر أمن المعلومات على أداء شركات في شركات التقنية بمدينة الرياض

المتغيرات المستقلة	معاملات الانحدار	قيمة اختبار T	مستوى الدلالة
المقدار الثابت	1.218	5.150	.000
الملموسية	.672	12.327	.000
معامل الارتباط = 0.759		معامل التحديد = 0.431	
قيمة الاختبار F = 151.957		القيمة الاحتمالية = 0.00	

يوضح الجدول أن مخاطر أمن المعلومات لها تأثير معنوي قوي على أداء شركات في شركات التقنية بمدينة الرياض . حيث أظهرت نتائج تحليل الانحدار قيمة اختبار T العالية لكل من المقدار الثابت (5.150) و الملموسية (12.327) مع مستوى دلالة 0.000، مما يشير إلى وجود علاقة دالة إحصائية. معامل الارتباط (0.759) يظهر علاقة قوية بين المتغيرات المستقلة وأداء شركات ، بينما معامل التحديد (0.431) يدل على أن 43.1% من التباين في أداء شركات يمكن تفسيره بواسطة المتغيرات المستقلة. وبناءً على قيمة الاختبار F (151.957) و القيمة الاحتمالية 0.00، فإن الفرض القائل بعدم وجود أثر دال إحصائياً يُرفض، مما يعني أن مخاطر أمن المعلومات تؤثر بشكل معنوي على أداء شركات

- الفرض الفرعي الثاني • لا يوجد أثر ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) لبعدهم مخاطر الاحتيال على أداء شركات في شركات التقنية بمدينة الرياض ..

للتحقق من صحة هذا الفرض تم استخدام تحليل الانحدار الخطي البسيط (Linear Regression test)، وجاءت النتائج كما بالجدول التالي:

جدول (11) أثر لبعده مخاطر الاحتيال على أداء شركات في شركات التقنية بمدينة الرياض ..

المتغيرات المستقلة	معاملات الانحدار	قيمة اختبار T	مستوى الدلالة
المقدار الثابت	1.268	7.116	.000
مخاطر الاحتيال	.693	16.141	.000
معامل الارتباط = 0.754		معامل التحديد = 0.566	
قيمة الاختبار F = 260.528		القيمة الاحتمالية = 0.00	

يوضح الجدول أن مخاطر الاحتيال لها تأثير قوي وذو دلالة إحصائية على أداء شركات في شركات التقنية بمدينة الرياض . أظهرت نتائج تحليل الانحدار الخطي البسيط أن المقدار الثابت و مخاطر الاحتيال لهما تأثير معنوي، حيث سجلت قيمة اختبار T لمخاطر الاحتيال 16.141 ومستوى دلالة (0.000)، مما يعني أن التأثير دال إحصائيًا. كما أن معامل الارتباط (0.754) يشير إلى علاقة قوية بين مخاطر الاحتيال وأداء شركات .معامل التحديد (0.566) يعني أن أكثر من نصف التباين في أداء شركات يمكن تفسيره من خلال مخاطر الاحتيال. بالإضافة إلى ذلك، قيمة الاختبار F (260.528) و القيمة الاحتمالية = 0.00 تؤكد أن النموذج ككل دال إحصائيًا. بناءً على هذه النتائج، يتم رفض الفرض الفرعي الثاني الذي ينفي وجود أثر لمخاطر الاحتيال على أداء شركات .

- الفرض الفرعي الثالث لا يوجد أثر ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) لبعده مخاطر عدم رضا العملاء على أداء شركات في شركات التقنية بمدينة الرياض .

للتحقق من صحة هذا الفرض تم استخدام تحليل الانحدار الخطي البسيط (Linear Regression test)، وجاءت النتائج كما بالجدول التالي:

جدول (12) أثر لبعد مخاطر عدم رضا العملاء على أداء شركات في شركات التقنية بمدينة الرياض

المتغيرات المستقلة	معاملات الانحدار	قيمة اختبار T	مستوى الدلالة
المقدار الثابت	.416	2.503	.013
مخاطر عدم رضا العملاء	.875	22.426	.000
معامل الارتباط = 0.847	معامل التحديد = 0.716		
قيمة الاختبار F = 502.914	القيمة الاحتمالية = 0.00		

يوضح الجدول أن مخاطر عدم رضا العملاء لها تأثير إيجابي قوي وذو دلالة إحصائية على أداء شركات في شركات التقنية بمدينة الرياض . سجل المقدار الثابت (0.416) قيمة اختبار T (2.503) مع مستوى دلالة (0.013)، مما يعكس تأثيراً معنوياً. كما أظهرت مخاطر عدم رضا العملاء معامل انحدار قوي (0.875) مع قيمة اختبار T (22.426) ومستوى دلالة (0.000)، مما يثبت أن لها تأثيراً دالاً على أداء شركات . معامل الارتباط (0.847) يشير إلى علاقة قوية بين مخاطر عدم رضا العملاء وأداء شركات ، في حين أن معامل التحديد (0.716) يعني أن 71.6% من التباين في أداء شركات يمكن تفسيره من خلال مخاطر عدم رضا العملاء . قيمة الاختبار F (502.914) مع القيمة الاحتمالية 0.00 تعزز من دلالة النموذج ككل. بناءً على هذه النتائج، يتم رفض الفرض الفرعي الثالث الذي ينفي وجود تأثير معنوي لمخاطر عدم رضا العملاء على أداء شركات .

الفصل الخامس : النتائج والتوصيات

1.5 نتائج الدراسة

ويتمثل ذلك في عرض أبرز النتائج التي توصل إليها البحث ، على النحو التالي:

أظهرت نتائج الدراسة أن متوسط تقييم "مخاطر أمن المعلومات" بلغ 4.10 مع انحراف معياري 0.91. هذه النتيجة تشير إلى أن المشاركين يوافقون بشكل كبير على فعالية تدابير أمن المعلومات في تعزيز أداء الشركات في شركات التقنية بمدينة الرياض. على الرغم من ذلك، يظهر الانحراف المعياري المرتفع وجود تباين نسبي في آراء المشاركين حول مدى تأثير هذه المخاطر على الأداء المؤسسي. تشير هذه النتيجة إلى أنه بينما يعترف الكثيرون بأهمية أمان المعلومات، قد لا يكون هناك توافق تام بين كافة المشاركين في مدى تأثيره.

وتتفق هذه النتيجة مع دراسة (Dorairajan (2024، التي أظهرت أن الأمن السيبراني يُعتبر عاملاً أساسياً في دعم الأداء التنظيمي للشركات من خلال تعزيز الثقة والكفاءة التشغيلية.

وسجلت "مخاطر الاحتيال" متوسطاً حسابياً قدره 4.11 مع انحراف معياري 0.91، مما يعكس موافقة قوية من المشاركين على أن هذه المخاطر تؤثر بشكل كبير على الأداء التنظيمي للشركات. تشير النتيجة إلى أن الشركات بحاجة إلى تكثيف استراتيجيات مكافحة الاحتيال المالي لضمان استقرار الأداء.

وتتفق هذه النتيجة مع دراسة (Quinn et al. (2023، التي أكدت على أهمية دمج مخاطر تكنولوجيا المعلومات والاتصالات (ICT) ضمن استراتيجيات إدارة المخاطر المؤسسية (ERM) لتعزيز قدرة المؤسسات على التعامل مع هذه المخاطر وتحسين الأداء المؤسسي.

وحصلت "مخاطر عدم رضا العملاء" على متوسط حسابي قدره 4.22 مع انحراف معياري قدره 0.80، مما يعكس توافقاً قوياً بين المشاركين حول أن هذه المخاطر تشكل تهديداً رئيسياً لأداء الشركات. يبرز

هذا التركيز على تحسين تجربة العملاء والحد من المخاطر المرتبطة بعدم رضاهم كإجراء استراتيجي حاسم لتحسين الأداء التنظيمي.

وتتفق هذه النتيجة مع دراسة (Hasan et al. (2021، التي أظهرت أن الشركات التي تهتم بسلامة بيانات العملاء وتوافر استراتيجيات موجهة نحو تحسين رضا العملاء يمكن أن تؤثر إيجاباً على الأداء المؤسسي.

2.5 نتائج اختبار الفرضيات

الفرضية الرئيسية: لا يوجد أثر ذو دلالة إحصائية عند مستوى $(\alpha \leq 0.05)$ للمخاطر الإلكترونية (مخاطر أمن المعلومات، مخاطر الاحتيال، مخاطر عدم رضا العملاء) على أداء الشركات في شركات التقنية بمدينة الرياض.

تم رفض هذه الفرضية بناءً على نتائج تحليل الانحدار المتعدد التي أظهرت وجود تأثير معنوي لجميع أبعاد المخاطر الإلكترونية على الأداء التنظيمي. إذ بلغ معامل الارتباط الكلي (0.897)، ومعامل التحديد (0.800)، مما يعني أن 80% من التغير في أداء الشركات يمكن تفسيره من خلال أبعاد المخاطر الإلكترونية. كما كانت قيمة اختبار $F = 160.304$ ودلالته 0.000، مما يدل على معنوية النموذج ككل، وتتفق هذه النتيجة مع دراسة (Hasan et al. (2021 التي أكدت أن جاهزية الأمن السيبراني تؤثر بشكل إيجابي ومباشر على الأداء المالي وغير المالي للمؤسسات، مما يوضح أن التعامل الجاد مع المخاطر الإلكترونية يعزز الأداء المؤسسي.

الفرض الفرعي الأول: تم اختبار الفرض القائل بعدم وجود أثر دال إحصائيًا لمخاطر أمن المعلومات على أداء الشركات. وقد أظهرت النتائج وجود تأثير دال، حيث بلغت قيمة اختبار $T = 5.150$ ، ومستوى الدلالة = 0.000، ومعامل التحديد = 0.431. وهذا يشير إلى أن مخاطر أمن المعلومات تفسر ما نسبته 43.1% من التباين في أداء الشركات، مما يدل على أن وجود تدابير غير كافية لحماية المعلومات يمكن أن يضعف من كفاءة الأداء المؤسسي.

وتتسق هذه النتيجة مع دراسة (Dorairajan (2024) التي أبرزت كيف أن تعزيز حماية سرية المعلومات وسلامة الأصول الرقمية يُعد من أهم محددات تحسين الأداء المؤسسي وتعزيز الثقة بين أصحاب المصلحة.

الفرض الفرعي الثاني اختبرت الدراسة أثر مخاطر الاحتيال على أداء الشركات، وأظهرت النتائج وجود تأثير معنوي قوي، حيث بلغت قيمة اختبار $T = 16.141$ ، ومستوى الدلالة $= 0.000$ ، مع معامل التحديد $= 0.566$ ، أي أن ما نسبته 56.6% من التغير في أداء الشركات يمكن تفسيره من خلال مخاطر الاحتيال. يشير ذلك إلى أن مؤسسات التقنية التي لا تدير مخاطر الاحتيال بشكل فعال قد تواجه تحديات مباشرة في تحقيق الاستقرار والكفاءة التشغيلية.

وتتوافق هذه النتيجة مع ما ورد في دراسة (Quinn et al. (2023) ، التي أوضحت أن دمج مخاطر تكنولوجيا المعلومات والاتصالات (ICT) ضمن برامج إدارة المخاطر المؤسسية (ERM) يؤدي إلى تحسين الوعي بالمخاطر وتخصيص الموارد بشكل فعال، مما يساهم في رفع مستوى الأداء المؤسسي.

الفرض الفرعي الثالث: أظهرت نتائج اختبار هذا الفرض أن لمخاطر عدم رضا العملاء تأثيراً قوياً وذو دلالة إحصائية على أداء الشركات، حيث بلغت قيمة اختبار $T = 22.426$ ، ومستوى الدلالة $= 0.000$ ، ومعامل التحديد $= 0.716$ ، مما يعني أن 71.6% من التغير في الأداء يمكن تفسيره من خلال هذا النوع من المخاطر. هذا يشير إلى أن تراجع رضا العملاء قد يكون له تأثير مباشر وفعال على أداء الشركات التقنية.

وتتفق هذه النتيجة مع دراسة (Dorairajan (2024) التي أكدت أن تعزيز تجربة العملاء وبناء ثقافة سيبرانية مسؤولة من شأنه أن ينعكس إيجاباً على الأداء التنظيمي ويزيد من التنافسية، وكذلك مع نتائج (Hasan et al. (2021) التي أظهرت أن الأداء الأمني الفعال يؤثر على كل من الأداء المالي وغير المالي، بما في ذلك رضا العملاء.

3.5 توصيات الدراسة:

استناداً إلى نتائج الدراسة المتعلقة بتأثير المخاطر الإلكترونية على أداء الشركات في شركات التقنية بمدينة الرياض، يمكن تقديم التوصيات التالية:

1. ينبغي على الشركات التقنية اتخاذ تدابير أمنية متقدمة لحماية البيانات الحساسة من الوصول غير المصرح به، بما في ذلك تطبيق تقنيات تشفير متطورة وتحديث الأنظمة الأمنية بشكل دوري لمواكبة التهديدات الحديثة.
2. تعزيز الوعي بالأمن السيبراني بين الموظفين على جميع المستويات من خلال برامج تدريبية دورية لتعريفهم بالتهديدات السيبرانية وكيفية التصدي لها.
3. يجب على الشركات التقنية تطوير استراتيجية شاملة لإدارة المخاطر الإلكترونية، تشمل تحليل المخاطر المحتملة ووضع خطط استجابة فعالة لتقليل تأثيرات المخاطر على الأداء.
4. توصي الدراسة بتطبيق سياسات وإجراءات قوية لمكافحة الاحتيال المالي، مثل تعزيز الرقابة الداخلية وتطبيق الأنظمة المتقدمة للكشف عن الأنشطة الاحتيالية في البيانات المالية.
5. ينبغي تخصيص موارد بشرية ومالية كافية لتنفيذ وتطوير نظم مكافحة الاحتيال، بما في ذلك استخدام أدوات تحليل البيانات للكشف عن الأنماط المشبوهة.
6. تعزيز تجربة العملاء لتقليل مخاطر عدم رضاهم، من خلال تحسين جودة الخدمة والمنتجات وتطوير قنوات التواصل الفعالة بين الشركة والعملاء.
7. يجب على الشركات تطبيق آليات لمراقبة شكاوى العملاء بشكل دوري، مع تقديم حلول سريعة وفعالة لحل المشكلات التي قد تؤثر على مستوى رضا العملاء.
8. توصي الدراسة بتشجيع الابتكار التكنولوجي داخل الشركات التقنية لتقليل تأثير المخاطر الإلكترونية على الابتكار وتعزيز القدرة التنافسية في السوق.
9. تبني سياسات تكنولوجية تساهم في تسريع اتخاذ القرارات الاستراتيجية وتقليل التأثيرات السلبية للمخاطر الإلكترونية على عمليات اتخاذ القرارات داخل الشركات.

10. يجب أن تضع الشركات في اعتبارها أهمية سمعتها في السوق وأن تسعى إلى تقليل المخاطر الإلكترونية

التي قد تؤثر على سمعة الشركة وتجذب العملاء الجدد.

11. توصي الدراسة بتطوير سياسات شاملة لإدارة الأزمات التي قد تنشأ نتيجة للمخاطر الإلكترونية، بما

في ذلك وضع خطط استجابة للطوارئ لضمان استمرارية العمل في حال حدوث اختراقات أمنية.

12. تعزيز التعاون بين الشركات التقنية والجهات التنظيمية المحلية والدولية لضمان الامتثال لأحدث

القوانين واللوائح المتعلقة بالأمن السيبراني وحماية البيانات.

Abstract

This study aimed to analyze the impact of electronic risks—represented by information security risks, fraud risks, and customer dissatisfaction risks—on the performance of companies within the technology sector in Riyadh, Saudi Arabia. To achieve the study's objectives, a descriptive-analytical approach was adopted. A total of 370 questionnaires were distributed to a simple random sample of employees working in tech companies in Riyadh, and 318 valid responses were retrieved, resulting in a response rate of 85.9%.

The results indicated that all three dimensions of electronic risks have a statistically significant impact on company performance. Among these, customer dissatisfaction risks were found to have the highest effect, followed by fraud risks, and then information security risks. The study recommended developing advanced information security policies, strengthening fraud detection systems, and improving customer relationship management to reduce dissatisfaction risks. It also emphasized the need to raise cybersecurity awareness at all organizational levels to ensure sustainable organizational performance in the evolving digital environment.

Keywords: Electronic risks, information security, cyber fraud, customer satisfaction, company performance, tech companies.

المراجع:

أولاً: المراجع العربية

- أحمد، مناف عبدالمطلب. (2019). أثر ممارسات إدارة الموارد البشرية الخضراء في تحسين أداء المنظمة: دراسة استطلاعية لأراء عينة العاملين في مستشفيات مدينة الرمادي. مجلة جامعة الأنبار للعلوم الاقتصادية والإدارية، مج 11، ع 26، 418 - 438. مسترجع من <http://search.mandumah.com/Record/1030585>
- أبو سعدة، آيات عبدالقادر بسيوني. (2024). أثر المنظمة المتعلمة على أداء العاملين: دراسة ميدانية على الشركة القابضة مصر للطيران. مجلة البحوث الإدارية، مج 42، ع 1، 1 - 40.
- أحمد، مناف عبدالمطلب. (2019). أثر ممارسات إدارة الموارد البشرية الخضراء في تحسين أداء المنظمة: دراسة استطلاعية لأراء عينة العاملين في مستشفيات مدينة الرمادي. مجلة جامعة الأنبار للعلوم الاقتصادية والإدارية، مج 11، ع 26، 418 - 438.
- أديب، أماني ألبرت. (2019). إدراك الشباب لمخاطر التسوق الإلكتروني داخل المجتمعات الافتراضية الاستهلاكية وعلاقته بسلوكهم الشرائي. المجلة المصرية لبحوث الرأي العام، مج 18، ع 1، 359 - 406. مسترجع من <http://search.mandumah.com/Record/1108207>
- بن عزة، محمد حمزة. (2018). حماية المستهلك الإلكتروني من مخاطر البريد الدعائي "Les Spamming": دراسة مقارنة. المجلة الأكاديمية للبحوث القانونية والسياسية، ع 4، 350 - 363. مسترجع من <http://search.mandumah.com/Record/1113496>
- تهامي، خالد صبيح الهادي. (2023). تأثير التمويل الأخضر على أداء المنظمة: الدور الوسيط للاستدامة المالية. مجلة البحوث التجارية، مج 45، ع 3، 227 - 271.
- الجرفي، محمد علي محمد عيسي، و التيجاني، مدثر حماد الشيخ. (2019). أثر تطبيق منهج المنظمة المتعلمة في أداء المنظمات: دراسة تطبيقية علي بنك سبأ الإسلامي بالجمهورية اليمنية (2014 م. - 2018 م.) (رسالة ماجستير غير منشورة). جامعة القرآن الكريم والعلوم الإسلامية، أم درمان.

- رشوان، أحمد محمد عبدالعال. (2020). تأثير الضغوط المؤسسية على أداء المنظمة: الدور الوسيط لممارسات سلاسل التوريد الخضراء: دراسة تطبيقية على قطاع الشركات الصناعية في مصر. مجلة البحوث المالية والتجارية، ع3، 952 - 983. - مسترجع من <http://search.mandumah.com/Record/1090653>
- رشوان، أحمد محمد عبدالعال. (2020). تأثير الضغوط المؤسسية على أداء المنظمة: الدور الوسيط لممارسات سلاسل التوريد الخضراء: دراسة تطبيقية على قطاع الشركات الصناعية في مصر. مجلة البحوث المالية والتجارية، ع3، 952 - 983.
- السيوف، سوار محمد عبدالرحمن، و الزبود، إسماعيل محمد عيد. (2019). مخاطر الألعاب الإلكترونية على الشباب: دراسة سوسيولوجية / طلبة الجامعة الأردنية (رسالة ماجستير غير منشورة). الجامعة الاردنية، عمان.
- صبيح، أميرة حسن سالم. (2021). مخاطر التسويق الرقمي عبر مواقع التسويق الإلكتروني وتأثيرها على أنماط السلوك الاستهلاكي لدى المراهقين. المجلة العلمية لبحوث العلاقات العامة والإعلان، ع22، 449 - 508. - مسترجع من <http://search.mandumah.com/Record/1218490>
- صميده، إيمان زكريا محمد، عطية، سماء طاهر مرسي، و غريب، منى محمد صالح. (2021). المعرفة الضمنية للعاملين وتأثيرها على تحسين أداء المنظمة: دراسة تطبيقية. مجلة البحوث الإدارية والمالية والكمية، مج1، ع1، 85 - 109.
- العازمي، عبدالله فالح خليفه عقيل، داود، ياسر إبراهيم محمد، و عمر، علاء الدين عبدالعزيز فهمي. (2022). دور تفعيل حوكمة تكنولوجيا المعلومات في تأمين المعلومات المحاسبية من المخاطر الالكترونية في ظل عصر الرقمنة: دراسة تطبيقية علي البنوك التجارية الكويتية. المجلة العلمية للدراسات والبحوث المالية والإدارية، مج13، ملحق، 1115 - 1155.
- عبدالعزيز، نوره السيد، عبدالسلام، محمد، عبدالسلام، إيمان محمد، و زايد، عادل محمد. (2024). أثر الذكاء الاستراتيجي على أداء المنظمة ريادة المنظمة متغير وسيط: دراسة ميدانية على احدى الشركات التابعة لوزارة الإسكان. مجلة التجارة والتمويل، ع4، 134 - 174.

- عزوز، على صلاح الدين، عبد الباري، علاء عبدالواحد، و المصري، ريم. (2018). أثر استراتيجيات تخفيض المخاطر المدركة للتسويق الإلكتروني على القرار الشرائي للمستهلك المصري: بالتطبيق على مواقع التواصل الاجتماعي (رسالة ماجستير غير منشورة). الاكاديمية العربية للعلوم والتكنولوجيا والنقل البحري، القاهرة. مسترجع من <http://search.mandumah.com/Record/965069>
- عزوز، على صلاح الدين، عبد الباري، علاء عبدالواحد، و المصري، ريم بهاء. (2019). أثر استراتيجيات تخفيض المخاطر المدركة للتسويق الإلكتروني على القرار الشرائي للمستهلك المصري: بالتطبيق على مواقع التواصل الاجتماعي. مجلة كلية التجارة للبحوث العلمية، مج56، ع2، 1، 25. - مسترجع من <http://search.mandumah.com/Record/1031861>
- غالى، بتول عبد علي. (2023). الحوكمة الالكترونية ودورها في تخفيض المخاطر الائتمانية من خلال تحسين القرارات المالية: دراسة تطبيقية لعينة من المصارف المدرجة في سوق العراق للأوراق المالية. مجلة رماح للبحوث والدراسات، ع88، 27، 59.
- غزال، فايز. (2022). تأثير الحوافز على الأداء في المنظمة: دراسة ميدانية على العاملين في شركة نسيج اللاذقية. مجلة جامعة تشرين للبحوث والدراسات العلمية - سلسلة العلوم الاقتصادية والقانونية، مج44، ع3، 141 - 157.
- فيصل، ثائر علي أحمد، و نور الدين، كباشي محمد حامد. (2018). الدور الوسيط لقدرات المنظمة في العلاقة بين تسويق الخدمات وتحسين أداء المنظمة: دراسة تطبيقية على المنظمات الخدمية بالخرطوم (رسالة ماجستير غير منشورة). جامعة النيلين، الخرطوم. مسترجع من <http://search.mandumah.com/Record/986413>
- المتولي، محمد محمود عبداللطيف. (2018). توسيط المخاطر المدركة في العلاقة بين مراجعات العملاء الإلكترونية ونية حجز الفندق في مصر: دراسة تطبيقية. المجلة العلمية للبحوث التجارية، ع5، 4، 171. 218. - مسترجع من <http://search.mandumah.com/Record/969793>

- مدانى، جميلة محمد. (2019). الإبداع في المنظمة الصناعية وأثره على أداء الأعمال: دراسة حالة الاقتصاديات الناشئة. مجلة المثقال للعلوم الاقتصادية والإدارية، مج5، عدد خاص ، 206. 189 -
مسترجع من <http://search.mandumah.com/Record/1027265>
- مصطفى، أنجي سمير محمود، الأحمدي، بسام محمد، و جبريل، ماجدة محمد. (2023). أثر تطبيق ممارسات التصنيع الأخضر على استدامة أداء المنظمة: دراسة تطبيقية على شركات الصناعات الغذائية. المجلة العلمية للاقتصاد والتجارة، ع4 ، 133 - 162.
- هاشم، عقيل قاسم. (2022). دور تحليل SWOT في تعزيز أداء المنظمة: دراسة تحليلية في وزارة العمل والشؤون الاجتماعية دائرة التقاعد والضمان الاجتماعي - بغداد. مجلة كلية الإدارة والاقتصاد للدراسات الاقتصادية والإدارية والمالية، مج14، ع2 ، 233 - 256.

ثانيا: المراجع الأجنبية

- Ahmed, Howaida Muhammad Lotfy, and Bahamdan, Nadra Saleh Muhammad Saeed. (2022). Saudi university youth's perception of potential risks from electronic marketing of pharmaceutical products: a field study. Journal of Middle East Public Relations Research, No. 37, 161-222. Retrieved from <http://search.mandumah.com/Record/1272005>
- Abed, A. L. A. (2020). The Impact of Learning Organization on Organizational Performance: An Empirical Study on Public and Private Commercial Banks in the Arab Republic of Egypt. Journal of Administrative Research, Vol. 38, No. 2, 1-21.
- Abu Wand, Rayana Amjad, and Abu Mughli, Azzam Azmi Masoud. (2023). The Influence of Entrepreneurship Practices on Organizational Performance: A Field Study in Commercial Banks in Amman (Unpublished Master's Thesis). Middle East University, Amman.

- Ahmed, A. A. H., and Badawy, S. M. (2024). Influence of Leadership Agility and Organizational Innovation on Organizational Performance. *Journal of the Higher Institute for Qualitative Studies*, Vol. 4, No. 5, 1543-1577.
- Al-Akroush, Marah Yasser, and Al-Sharbaty, Abdulaziz Ahmed. (2023). The Impact of Organizational Agility on the Organizational Performance at Jordanian Commercial Banks (Unpublished Master's Thesis). Middle East University, Amman.
- Balishani, Waheeba. (2021). The Risk of Electronic Shopping on Consumer Attitudes. *Journal of Entrepreneurship for Business Economics*, Vol. 7, No. 3, 339-356.
- Balishani, Wahiba. (2021). The Risk of Electronic Shopping on Consumer Attitudes. *Al-Reyadah Journal of Business Economics*, Volume 7, No. 3, 339-356. Retrieved from <http://search.mandumah.com/Record/1206285>
- Barbary, W. F. (2020). The Relationship between Business Process Management and Organizational Performance: An Applied Study on Telecom Egypt. *Journal of the Future of Social Sciences*, Vol. 2, No. 1, 3-40.
- Dorairajan, V. (2024, July). Cybersecurity and Organisational Performance—the Interplay. In *ARPHA Conference Abstracts* (Vol. 7, p. e129255). Pensoft Publishers.
- Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications*, 58, 102726
- Hussein, Abdullah Talib Abdullah, and Al-Naimi, Muhammad Abd al-Aal Amin. (2019). The Impact of Dynamic Capabilities on Organizational Performance: Examining the Mediating Effect of Strategic Fit and the Moderating Effect of Organizational Learning (Unpublished Master's Thesis). University of Jordan, Amman.

- Maamari, Muhammad. (2022). Modern approaches to improving performance in the organization: the Kaizen model. *Journal of Detective Notebooks*, Volume 17, Issue 1, 33-47. Retrieved from <http://search.mandumah.com/Record/1276695>
- Mohammed, A. A. B., and Ibrahim, E. H. A. M. (2024). The Role of Continuous Auditing in Reducing the Risks of Electronic Publishing of Financial Reports: A Field Study on the National Audit Bureau. *Scientific Journal of Business and Environmental Studies*, Vol. 15, No. 2, 65-89.
- Qaisi, S., and Zeroug, Y. (2023). Insurance in the Face of Informational Development: Electronic Insurance Contracts and Electronic Risk Insurance. *Journal of Legal and Social Sciences*, Vol. 8, No. 3, 151-169.
- Redjem, K., and Ouddane, B. (2022). The Impact of the Risk of Electronically Processing Accounting Data on the Quality of the Auditor's Reports External: Case Study of External Auditor in Ouargla-Algeria. *Journal of Financial, Accounting and Administrative Studies*, Vol. 9, No. 2, 219-235.
- Stephen, Quinn., Nahla, Ivy., Matthew, Barrett., Larry, Feldman., Daniel, Topper., Greg, Witte., Karen, Scarfone., Robert, H., Gardner., Julie, Chua. (2023). Enterprise Impact of Information and Communications Technology Risk:. doi: 10.6028/nist.sp.800-221
- Yahya, Gamal Ibrahim, Al-Zaq, Yahya Shahata, and Al-Sawalehi, Haitham Abdel-Razeq. (2024). The Impact of Organizational Inertia on Organizational Performance in Travel Agencies and Hotels: The Moderating Effect of Organizational Agility. *Journal of the Faculty of Tourism and Hotels*, Vol. 8, No. 1, 325-345.
- Zakandariya, Houria. (2016). The role of training in improving the organization's performance. *Al-Hikma Journal of Social Studies*, No. 7, 157-170. Retrieved from <http://search.mandumah.com/Record/769769>.

الملاحق

استمارة استبيان

السلام عليكم ورحمة الله وبركاته

أخي الكريم / أختي الكريمة

تحية طيبة وبعد،

يقوم الباحثين بإجراء دراسة حول قياس أثر المخاطر الالكترونية على أداء المنظمة "دراسة تطبيقية على شركات التقنية بمدينة الرياض"

ونظراً لما لديكم من المعرفة العلمية والخبرة العملية ذات الصلة بموضوع البحث، نأمل الحصول منكم على العون والمساعدة في توفير المعلومات المناسبة لأغراض البحث، من خلال التكرم بإبداء رأيكم بالتأشير على الإجابة المناسبة من وجهة نظركم.

وأقدم لحضراتكم بجزيل الشكر والتقدير للمساهمة في جهدكم في تعبئة هذا الاستبيان علماً أن جميع البيانات التي سيتم الحصول عليها منكم ستعامل بسرية تامة، ولن تستخدم لغير أغراض هذا البحث، وسوف أزودكم بنتائج هذه الدراسة حال اكتمالها إن شاء الله.

وتفضلوا بقبول فائق التقدير والاحترام

أولاً: البيانات الشخصية

- 1- النوع الاجتماعي ☐ ذكر ☐ أنثى
- 2- العمر ☐ 30 سنة فأقل ☐ من 40 - 30 سنة ☐ من 50 - 41 سنة ☐ من 50 سنة فأكثر
- 3- المستوى التعليمي ☐ ثانوي فأقل ☐ بكالوريوس ☐ ماجستير ☐ دكتورة
- 4- سنوات الخبرة ☐ 5 سنوات فأقل ☐ من 5 - 10 سنة ☐ من 15 - 11 سنة ☐ أكثر من 15 سنة
- 5- المهني الوظيفي ☐ إداري ☐ هندسي ☐ تقني ☐ أخرى

ثانيا محاور الاستبيان

✿ المحور الأول: المخاطر الإلكترونية ، ضع إشارة (✓) في المربع المناسب لاختيارك:

المبعد	أوافق بشدة	أوافق	محايد	معارض	معارض بشدة
مخاطر أمن المعلومات					
تحيي المعلومات من الوصول غير المصرح به، مما يضمن سرية البيانات ويحافظ على خصوصية الأفراد والمؤسسات.					
يستخدم تقنيات تشفير فعالة لضمان حماية البيانات الحساسة، مما يمنع تسريب المعلومات أثناء انتقالها عبر الشبكات.					
يطبق أنظمة أمنية لحماية الشبكات من الهجمات الخارجية، مما يساهم في تقليل خطر الاختراقات والتهديدات المتزايدة.					
يحدث الأنظمة الأمنية بشكل دوري لمواكبة التهديدات الحديثة، الأمر الذي يعزز القدرة على التصدي للمخاطر الإلكترونية المستجدة.					
يوفر برامج تدريبية للموظفين بشأن مخاطر أمن المعلومات، مما يعزز وعيهم ويؤهلهم للتعامل مع التهديدات الإلكترونية بفعالية.					
مخاطر الاحتيال					

					تحديد الأساليب الاحتمالية الحديثة التي قد تهدد النظام المالي
					تعزيز السياسات والإجراءات لمكافحة محاولات الاحتيال المالي
					مراقبة الأنشطة المشبوهة داخل الأنظمة المالية لرصد الاحتيال
					تطبيق أنظمة متقدمة للكشف عن الأنشطة الاحتمالية في البيانات المالية
					توفير برامج تدريبية مستمرة للموظفين حول أساليب الاحتيال وطرق مكافحتها
مخاطر عدم رضا العملاء					
					تحديد العوامل التي تؤدي إلى عدم رضا العملاء وتحليل تأثيرها على السمعة المؤسسية
					تحسين جودة الخدمة المقدمة للعملاء لتقليل احتمالات عدم رضاهم
					مراقبة شكاوى العملاء بشكل دوري وتقديم حلول سريعة وفعالة
					تعزيز قنوات التواصل مع العملاء لضمان فهم احتياجاتهم ومتطلباتهم
					توفير استراتيجيات للتعامل مع الشكاوى والعمل على تحسين الخدمة بناءً عليها

✿ المحور الثاني: أداء الشركات ، ضع إشارة (✓) في المربع المناسب لاختيارك:

معارض بشدة	معارض	محايد	أوافق	أوافق بشدة	البعد
					تؤثر المخاطر الإلكترونية على قدرة المنظمة على تحقيق أهدافها الاستراتيجية بشكل سلبي.
					تعرض الشركة للمخاطر الإلكترونية يعيق بشكل ملحوظ تحسين كفاءة العمليات الداخلية.
					تؤدي المخاطر الإلكترونية إلى زيادة التكاليف التشغيلية بسبب استجابة المنظمة للحوادث الأمنية.
					تؤثر المخاطر الإلكترونية بشكل مباشر على الابتكار في منتجات أو خدمات الشركة.
					تؤدي المخاطر الإلكترونية إلى تباطؤ في اتخاذ القرارات الاستراتيجية داخل المنظمة.
					تؤثر المخاطر الإلكترونية بشكل سلبي على رضا العملاء والعلاقات مع الموردين.
					تؤدي المخاطر الإلكترونية إلى تأخير أو توقف في تحقيق الأهداف المالية المحددة.
					يؤدي التعامل غير الفعال مع المخاطر الإلكترونية إلى انخفاض في إنتاجية الموظفين.

					المخاطر الإلكترونية تؤثر على سمعة الشركة في السوق وبالتالي تقلل من قدرتها على جذب العملاء الجدد.
					تؤدي المخاطر الإلكترونية إلى تأثير سلبي على ثقافة العمل داخل المنظمة.

مع خالص التقدير والاحترام

Mid-Ocean University

College of Management

Department of risk management



**The impact of electronic risks on organisational
performance: An applied study on technology companies in
Riyadh.**

Preparation:

Ammar Fahad Al-Tamimi

242001099

Supervision:

Dr. Emad Al-Nakhly

1446 – 2025